Trustix™

Trustix Enterprise Firewall 4.6
User Guide

Revision 1.9 08-07-2005

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS USER GUIDE ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS USER GUIDE ARE BELIEVED TO BE ACCURATE, BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET SHIPPED WITH THE PRODUCT, AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT COMODO TRUSTIX OR A COMODO TRUSTIX REPRESENTATIVE FOR A COPY.

Copyright © 2005 by Comodo Trustix Limited.

All rights reserved. No part of the contents of this user manual may be reproduced or transmitted in any form or by any means without prior written permission of Comodo Trustix Limited.

Trustix and XSentry are trademarks of Comodo Trustix Limited. All other brands and product names are trademarks or registered trademarks of their respective holders.

Contact information:

COMODO TRUSTIX LIMITED,
NEWCOURT,
REGENTS PLACE,
REGENTS ROAD,
MANCHESTER,
M5 4HB
UNITED KINGDOM

or visit the web site at http://www.trustix.com

e-mail : trustix@trustix.com

Trustix™

Contents

Chapter 1

Concepts 1

Firewall 1

Number of Zones 3

Network Device 3

TCP/IP 3

Addressing Issues 4

Routing 4

Gateway 5

Subnetting 5

Port addressing 5

Destination Network Address and Port Translation 5

Source Network Address Translation 6

Virtual Private Networking (VPN) 6

IPSec 7

How Does the Firewall Work? 7

Understanding Rules and Rule Setting 7

Types of Rules 8

Entities 8

Logging 9

Dynamic IP Address Allocation 10

Pre-defined Services 10

Custom Designed Services 10

Preface and Quick Start 11

Quick Start Guide 11
Part 1: Installation 11
Part 2: Licensing 18
What's new in Trustix Enterprise Firewall 4.6 21
What's new in Trustix Enterprise Firewall 4.1 24
What's new in Trustix Enterprise Firewall 4.0 25
What is new in Trustix Enterprise Firewall 3.5 25
Firewall Overview 27
About this User Guide 29
Conventions 29
Additional Resources 29

Chapter 2
Firewall Server Installation 31
Pre-installed Firewall Server 31
Prerequisites 31
System Requirements 32
Firewall Server 32
Firewall Client 33
Firewall Server Installation 33
Preparation 33
Installation 33
Checklist: 33
Booting Up 34
Keyboard Setup 34
Patitioning the hard disk 35
Network Settings 37
Host Configuration 38
Remote Configuration 40
Finalising the installation 40

Chapter 3
First-time Configuration of Firewall 41
Console Configuration 41

Firewall Console 42
Configuring the Firewall Console 44
Setting the LAN Interface 45
Setting the Zone Names 45
Setting Gateway 46
Define Remote User 46
Physical Installation 48
Locating the LAN Network Device 49
Shell 50
Installing the Firewall Client 50
Installing the Windows Firewall Client 51
Installing the Linux Firewall Client 51
De-installing the Windows Firewall Client 53
De-installing the Linux Firewall Clients 53
Installing the Firewall License 54
General Licence Issues 54
Getting the Licence Key 54

Chapter 4
Using the Firewall Console 57
System Password 57
Menu Administration 58
Change System Password 59
Edit Firewall Users 60
Re-enable Blocked Administration Hosts 61
Configure Administration Host Blocking 61
Configure Networks 62
Set Default Gateway 62
Set LAN Interface 63
Set Name Server 63
Configure Filtering Proxy 64
Configure Traffic Control 64
Failure Notification 65

Upgrade Server 66
Shutdown Firewall 66
Block/Unblock Traffic 67
Enable/Disable Ping Testing 67
Enable/Disable Remote SSH 68
Set Keyboard Layout 69
Set Time Zone 70

Chapter 5
The Firewall Client 71
Starting the Firewall Client 71
The Client Window 71
The Menu Bar 72
Application 72
Firewall 75
Help 75
The Toolbar 75
The Work Area 76
Worksheet 76
The Network View 79

Chapter 6
The Firewall Administration Application 81
Start-up 81
Configuration Basics 82
Operations 82
Adding a Node 82
Adding a Host 83
Adding a Service 83
Adding a Server 84
Adding a Subnet 85
Adding a Server Class 85
Adding Host Folder 86
Adding VPN 87

Removing a Node 89
Changing the Properties of a Node 89
Setting Rules 90
Changing the Properties of a Rule 92
Deleting Rules 93
Activating Rules on Firewall 93
Save Configuration 93
Enable Logging on Rules 93
Rule Examples 93
The Use of Service 93
The Use of Hosts 94
The Use of Host Folders 96
The Use of Servers 96
The Use of Subnets 97
The Use of Server Class 98
The Use of Source NAT 99
The Use of Destination NAPT 101
Advanced Options 102
Services 102
Create a New Service 103
Editing an Existing Service 105
LAN Client Configuration 106
MS Windows 95/98 106
MS Windows NT 4.0 108
MS Windows 2000 110
Linux 112

Appendix A
Firewall Rules and Policy 113

Appendix B
Using ssh in MS Windows 115

Appendix C
Predefined Services 117

Services and Port Ranges 120

Appendix D

Upgrading the Firewall 123

Security when Upgrading 123

How to Upgrade 123

Preparations before Upgrade 124

Appendix E

Console Tools on the Firewall 125

fwlogwatch 125

Appendix F

VPN and Road Warriors 127

Virtual Private Network 127

Digital Certificates 127

Road Warriors 129

Considerations when Allowing Road Warriors 129

The Network 129

The Pass Phrase 130

The Road Warrior's Computer 130

Managing the Certificates 130

Using Road Warrior Functionality in the Firewall 131

Creating Certificates 131

Connecting to a Firewall 133

Adding Road Warriors to the Worksheet 134

Revoking Certificates 136

Available third-party VPN clients 136

Interoperability 136

Appendix G

Virtual LAN 137

Concept 137

Client Side Virtual LAN - java client 137

Add VLAN 138

Modify VLAN 138
. 139
Remove VLAN 139
Server Side Virtual LAN - xsadm console 140
Add VLAN 141
Modify VLAN 141
Deleting VLAN 142

Appendix H
Traffic Shaping 145

Appendix I
Microsoft Exchange Servers 149
Allowing MAPI Client Access through a Firewall: 150

Appendix J
Licences 151
Trustix Secure Linux Products 151
LICENSE AGREEMENT 151

Appendix K
Trustix Technical Support 157
Premium Technical Phone Support 157

Appendix L
DHCP Server and Relay Support 159
DHCP Server 159
DHCP Common 159
IP Pools 160
Static Host 161
DHCP Relay 163

Appendix M
Monitoring and Alerts 165
Monitoring 165
Alerts 167

Adding Alerts 167
Deleting Alerts. 168
Editing Alerts 168

Appendix N
Network Configuration 171
Devices Configuration. 171
Gateway Configuration 172
LAN Configuration 173
DNS Configuration 174
Hosts Configuration 175

Appendix O
ARP Proxy 179
. . . . . Add ARP Proxy179
. . . . . Edit ARP Proxy180
. . . . . Delete ARP Proxy180

Appendix P
Advanced Logging 181
Display Configuration 181
LogRotate Configuration 182
Firewall Log Search 183
System Log Search 186

Appendix Q
Static Routing 191
Adding Static Routing 191
Removing Static Routing 192

Appendix R
Firewall Policies within a Subnet 193

Appendix S
Xsadm console menu option from Java GUI 195
Change System Password 195

Blocked Admin Hosts 196
Configure Admin Host Blocking. 196
Enable Traffic Control 197
Disable Traffic Control. 198
Failure Notification e-Mail. 199
Upgrade Server. 199
Shutdown Firewall 200
Block Traffic 200
UnBlock Traffic 201
Enable Ping Testing 202
Disable Ping Testing 203
Disable Remote SSH. 204
Enable Remote SSH 205
Disable License Negotiating 206
Enable License Negotiation 207

Appendix T

User Management 211

New User. 211
Edit User 212
. 214

Appendix U

High Availability 203

Concept. 203

Index 207

Trustix™

Chapter 1

Concepts

This chapter explains terms that are used in the Firewall, important concepts regarding networking and the firewall, and how different network entities are used and operated in order to visually implement the security policy in the Firewall. It is important that this chapter is studied thoroughly.

Firewall

The firewall should be placed as the only link between the local network and the connection to the Internet. (Figure 1-1 & Figure 1-2)

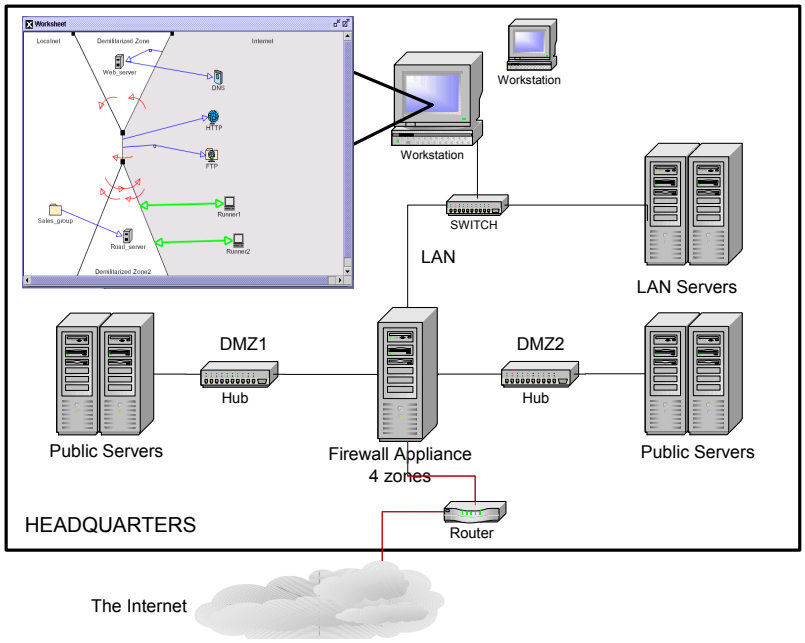


Figure 1-1 Firewall implementation with four zones.

Notice the following elements:

- *LAN* – Local Area Network. The organization's local network that is protected by the Firewall.
- *The Internet* - A worldwide network of computer networks. The Internet represents the *external network*, which the LAN is protected from. The external network does not have to be the Internet; it can be any IP-network. The user guide is written assuming that the external network is the Internet.
- *DMZ* - Demilitarized zone or secure zone. A network where public services, like web servers should be placed. Using a demilitarized zone increases security on the LAN. The LAN and the public services will not be on the same network, minimizing the risk of intrusion via publicly accessible services. Although the usage of a DMZ is not necessary for providing services to the Internet, it is highly recommended. Depending on license, the Firewall supports several DMZs. A second or third DMZ adds a higher degree of security to the network.

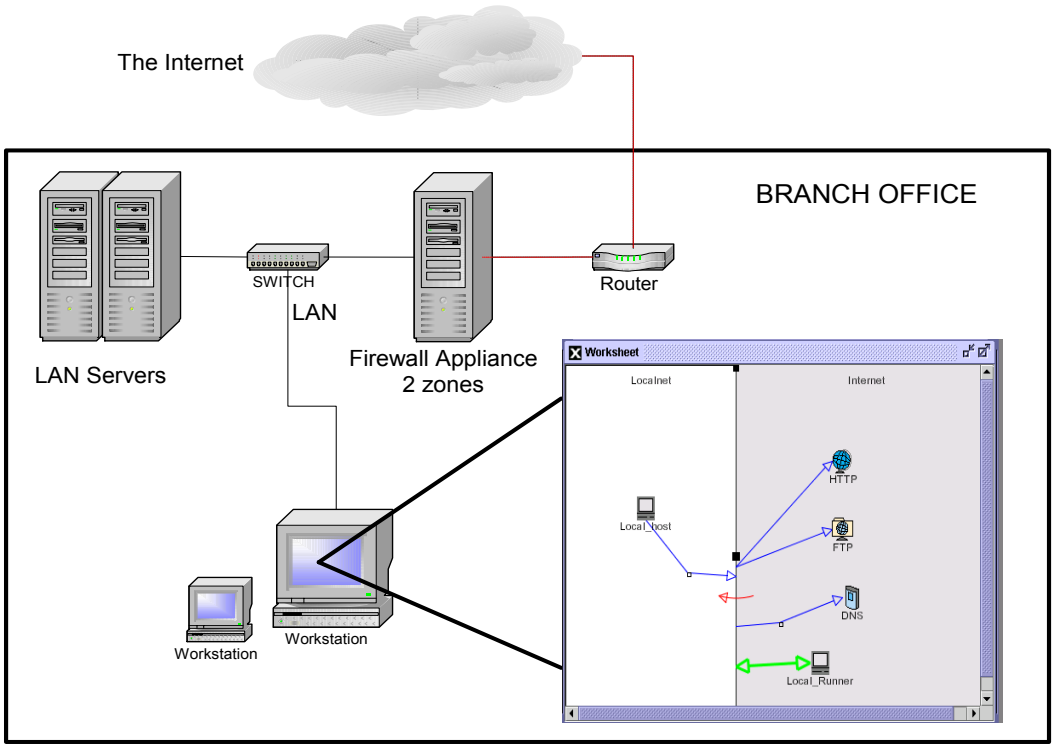


Figure 1-2 Firewall implementation with two zones.

Number of Zones

Two Zones: LAN and the Internet. For companies that do not need their servers accessible from a public network, and therefore need no secure zone. Such companies often receive web and mail services from their ISP.

Three zones: LAN, the Internet and secure zone. For companies which e.g. have their own web and mail servers.

Four zones: LAN, the Internet and 2 secure zones (working like Demilitarized Zones for the company). For companies which e.g. want to separate outgoing and incoming traffic. It can also be set up with a second LAN to gain a higher degree of traffic control on the local network.

Multiple zones: In addition to what is described above, additional zones can be used by large organizations wishing to give e.g. each department a separate security zone. Schools and universities may also want to define classrooms/computer labs as separate zones.

Network Device

A network device is a supported *network interface card* installed on the firewall. The Firewall requires at least two installed network devices. If one/two secure zones are used, three/four network devices are required. Each network device is attached to one network and needs an address on that particular network. The network devices are referred to as eth0, eth1, eth2 and eth3 in the Firewall.

TCP/IP

When computers are communicating, they need to speak the same language. In the world of computer networking, the languages are defined in protocols. The *Internet Protocol* (IP) is a protocol used on the Internet and in Local Area Networks (LANs).

The Internet Protocol, is the specification of the *IP-packet*, the basic communication unit on the Internet. An IP-packet can be compared to an ordinary letter. When a computer wishes to send data to another computer, it sends the data inside IP-packets. All IP-packets have source- and destination addresses. This means that every computer which whishes to communicate has to have an address, an IP address. An *IP-address* is a number that uniquely identifies a computer on an IP network. In fact, it is a number that uniquely identifies a network device, since a computer can have several devices connected to different networks.

IP handles sending data from one computer to another, but what the user wants is to have a program communicate with a program on the destination computer. This is handled by transport protocols like *Transmission Control Protocol* (TCP) and *User Datagram Protocol* (UDP).

Addressing Issues

An IP address is a number that uniquely identifies a computer on an IP network. IP addresses are written as 4 numbers, separated by dots. E.g.: 192.168.0.1

Each number can be in the range from 0 to 255. The IP address consists of a *network part*, and a *host part*. The range of available addresses has been divided into three types of networks. Class A, B and C. The classes can hold 16 million, 65 thousand and 254 addresses respectively.

On all IP networks there are special addresses. The *network address*, which identifies the network, and the *broadcast address* that is used to send packets to all addresses on a network.

If TCP/IP is used in a local area network, the system administrator manages the IP addresses used, and ensures that no duplicates are used. Computers connected to the Internet have to use IP addresses assigned from *Network Information Center* (NIC) an organization, which manages all IP addresses in the world to avoid conflicts. Determining what addresses to use can be a complex process. It is beyond the scope of this user guide to address all aspects of this process. Normally *Internet Service Providers* (ISPs) provide organizations with IP addresses. They can often provide guidance in the configuration process as well.

Routing

Routing is the process of sending data from a host on one network to a host on another network through a router. A *router* is a device that is connected to several networks. Its job is to determine what network data should be forwarded and then forwards it. A router can be thought of as a post office. When IP-packets are coming in, the packets are sorted, and sent to the destination post office. The last post-office delivers the packet to the recipient. In addition to functioning as a firewall, the Firewall will act as a router between all networks connected.

Gateway

In this context, the *gateway* is the router, which connects the LAN to the Internet. If a computer on the LAN wishes to send data to a computer on the Internet, it should send the data to the network gateway. The gateway then routes the data to the destination. The Firewall will be the gateway for the LAN and the secure zone. All computers on the LAN and the secure zone that are going to contact other computers on the Internet need to know the address of the gateway.

To know where to route traffic further, the Firewall also needs to have a gateway. The Firewall's gateway address should be an address to a router connected to the external network. In most cases, the ISP will provide this address.

Subnetting

Subnetting is the process of splitting an IP network into several subnetworks for internal use, while still acting like one network to the outside world. There are several cases where using subnets should be considered.

Port addressing

TCP and UDP use port addressing to deliver packets to the relevant application layer services. A port address is a 16-bit number. Port numbers below 1024 are called 'well-known ports' and uniquely identify the machine's most common application layer services, such as FTP, HTTP, TELNET and SSH.

Examples of well known ports are: port 22: SSH, port 23: telnet, port 80: HTTP.

Destination Network Address and Port Translation

A firewall can use port address translation, or *port forwarding*, to hide these well known ports on a machine from the public network by giving the ports other port numbers belonging to a machine on the LAN or secure zone. The firewall receives a packet to a well-known port and dispatches the packet to the corresponding port on the inside.

The firewall can also do IP address translation, so that the real IP address of a server behind the firewall is hidden from the outside world. This can be done at the same time as port translation.

When setting rules for port forwarding the administrator needs to be aware of port 350. For security reasons the Trustix Firewall uses this port for remote SSH instead of port 22, which is standard. If, for some reason, the administrator wishes to use port forwarding to another service which runs on port 350, the port for the SSH daemon must be changed first. This is done by logging on to the firewall with `ssh` on port 350 and change the port in the file `/etc/ssh/sshd_config`. Afterwards the service has to be restarted with the command

```
$ service sshd restart
```

Source Network Address Translation

Source Network Address Translation (source NAT) is the process of having the Firewall function as a gateway to the Internet for computers on a LAN, while hiding their real network addresses from the destination computers.

When a computer on the LAN wishes to contact a computer on the Internet, it sends the message to the Firewall, which then substitutes the source address with its own IP address (known as masquerading), or another chosen address, before forwarding it. When the response is coming, the Firewall replaces the destination address and forwards it back to the correct receiver on the LAN.

Virtual Private Networking (VPN)

VPN uses a public network, such as the Internet to create a secure, encrypted, private network connecting companies, and their business associates. In the Firewall, secure connections are created between two networks. Everything passing through the public net is encrypted by the *IP Security Protocol* (IPSec) gateway machine and decrypted by the gateway at the other end.

The Firewall supports VPN connections between two Firewalls. This enables companies with decentralized offices to set up secure encrypted VPN tunnels between their offices, using Internet as a transport layer instead of leasing permanent lines between the offices.

For more information about setting up VPN-connections with 3rd-party client applications, please refer to "VPN and Road Warriors" on page 127.

IPSec

The *Internet Security Protocol* (IPSec) is an extension of the IP protocol. It is designed by the Internet Engineering Task Force to provide end-to-end security for packets traveling over the Internet. IPSec predominantly implements the three basic areas of securing the Internet Protocol, authentication algorithms, encryption algorithms and key management.

In the Firewall, IPSec is used for creating Virtual Private Networks (VPNs).

How Does the Firewall Work?

To separate networks from each other, the Firewall uses a technique called *IP filtering*. When data is sent from one computer to another, it is in the form of IP packets. An IP packet consists of two parts, the *headers* and the *data*. The headers include control data such as destination and source address. IP-filtering is a process where each packet of data that arrives at the firewall is inspected. The headers of the IP-packets are checked against rules set by the network administrator for what traffic should be allowed, and the firewall then either allows or denies the packet to be forwarded depending on these rules. In addition to IP-filtering, the Firewall can be configured to use masquerading to further secure the local network.

Understanding Rules and Rule Setting

Rules are the most essential components of the firewall configuration. They are used by the firewall to decide what data should be forwarded and what data should be denied. It is therefore necessary to understand the properties of rules.

A rule consist of the following:

- Type (Action)
- Source entity
- Destination entity

Types of Rules

There are five types of rules: *allow, masquerade, deny, port forward* and *VPN tunnel*.

- *Allow* – The type of traffic specified in the rule should be *forwarded* by the firewall.
- *Source Network Address Translation* – The type of traffic specified in the rule should be *forwarded* by the firewall, after the real source address has been translated.
- *Deny* – The type of traffic specified in the rule should *not be forwarded* by the firewall.
- *Destination Network Address and Port Translation* – The type of traffic specified in the rule should be *routed* to another host address and/or port number on the company's network.
- *VPN tunnel* – All traffic between the LAN and a gateway or "road warrior" must go through a VPN connection. This rule can be set from a VPN gateway. Note that all traffic from this zone with destination for the subnet behind the gateway will go through the VPN tunnel. This also applies for traffic to a road warrior's virtual IP.

Entities

The source and destination entity of a rule is either a zone or a node. There are several different types of nodes. Understanding the differences in properties between these nodes is necessary in order to implement the organization's security policy with the Firewall.

Zone

A zone represents a network. Each zone is linked directly to a network device on the firewall. A zone is used to set rules for the corresponding network. E.g., deny all traffic from the Internet zone to the LAN zone.

Node

There are 9 types of nodes: *service, servicefolder, host, host folder, server, server class, subnet*, *VPN Gateway* and *roadwarrior*. Nodes are added to zones, and are closely attached to them.

- *Service nodes* are used for blocking or opening for a specific network service to a zone. The most common services come pre-defined with the Firewall, and

others can be added manually. E.g., the LAN should be able to access all web sites on the Internet.

- *Service folder nodes* are used if you need to set the same rule to a collection of services.
- *Host nodes* are used for blocking or opening for all traffic to/from one host. E.g., the host 192.168.0.1 on the LAN should be able to access the Internet.
- *Host folders* are simply collections of hosts. They make it easier to set the same rules from or to many hosts at the same time.
- *Server nodes* are used for specifying rules to specific services on one computer. E.g., the LAN should be able to access the web server on one specific host.
- *Server class nodes* are used if an organization has many servers with the same properties. E.g., 20 web servers placed in the secure zone should be accessible from the Internet zone and have access to the DNS service in the Internet zone.
- *Subnet nodes* are used for allowing/denying traffic from/to entire subnets.
- *VPN Gateway* is a remote server acting as the remote entrance to a VPN tunnel that opens into a zone on the firewall.
- *Road Warrior.* The Road warrior is a travelling person who needs a secure connection to the firewall. This is achieved by running 3rd-party software (described in "VPN and Road Warriors" on page 127).

Nodes can be given names, which help identifying them. These names must not be confused with DNS names.

Logging

Logging is the process of recording events that occur. An event can be anything from the denial of a packet to simply detecting the addition of a new rule. The events generate log entries, which are written to a log file. The log can later be used to discover and document possible break-in attempts or simply watching the traffic flow. Thus, the log contains both security information and information about the network traffic in general.

Dynamic IP Address Allocation

IP address allocation servers are often used in LANs. The system administrator assigns all IP addresses to an IP address allocation server (E.g. DHCP or BOOTP). Each time a computer on the LAN starts up, the TCP/IP software requests an IP address from the server. The server replies with an address. IP address allocation servers can be configured to dynamically allocate IP numbers. When this is done, the computers on the network can have different IP addresses for each time they are restarted. This has the following impact on the Firewall:

- For security, the Firewall can only be administered from computers that have IP addresses the firewall recognizes. These IP addresses have to be set in the firewall console. If dynamic IP address allocation is used on the LAN, the administrator computers cannot be configured to use this service. The administrating computers must have a static IP address.
- Setting rules on nodes that has obtained their IP addresses from a DHCP server will have no meaning.

Pre-defined Services

Pre-defined services are protocols and services that we have found are the most used services on the Internet. For a complete list of the services, please read "Predefined Services" on page 117 for more information.

Custom Designed Services

It is possible to define your own custom services in the Firewall. Please refer to "The Firewall Administration Application" on page 81 for instructions on how to define new services. Specifications of services will also become available at the Trustix web site.

Trustix™

Preface and Quick Start

Welcome to Trustix Enterprise Firewall, the new generation network firewall with a unique graphical interface for firewall administration. Trustix Enterprise Firewall allows users to rapidly develop a graphical representation of their networks, and then work with this model on their desktop in order to graphically define security policies.

The Trustix Enterprise Firewall is firewall administration made easy, and at the same time very secure. With Trustix Enterprise Firewall, users do not have to be troubled with editing complex sets of rules in order to define security policies. Users simply work with the graphical representation in the firewall client.

We recommended that you study this guide before installing the firewall. The user guide introduces the Firewall and provides the information needed to get everything installed and running. It gives answers to common questions and describes where to find more information.

Trustix Enterprise Firewall is based on Trustix XSentry software.

Quick Start Guide

Part 1: Installation

This guide will help you to install, license and set up basic rules on your Trustix Firewall.

Checklist:

PC-compatible computer for the firewall.

Trustix Enterprise Firewall CD

License certificate for the Firewall

IP address settings for your network:

Gateway IP address

Nameserver IP addresses

IP address settings for each network card (zone)

IP address of the administrator's machine

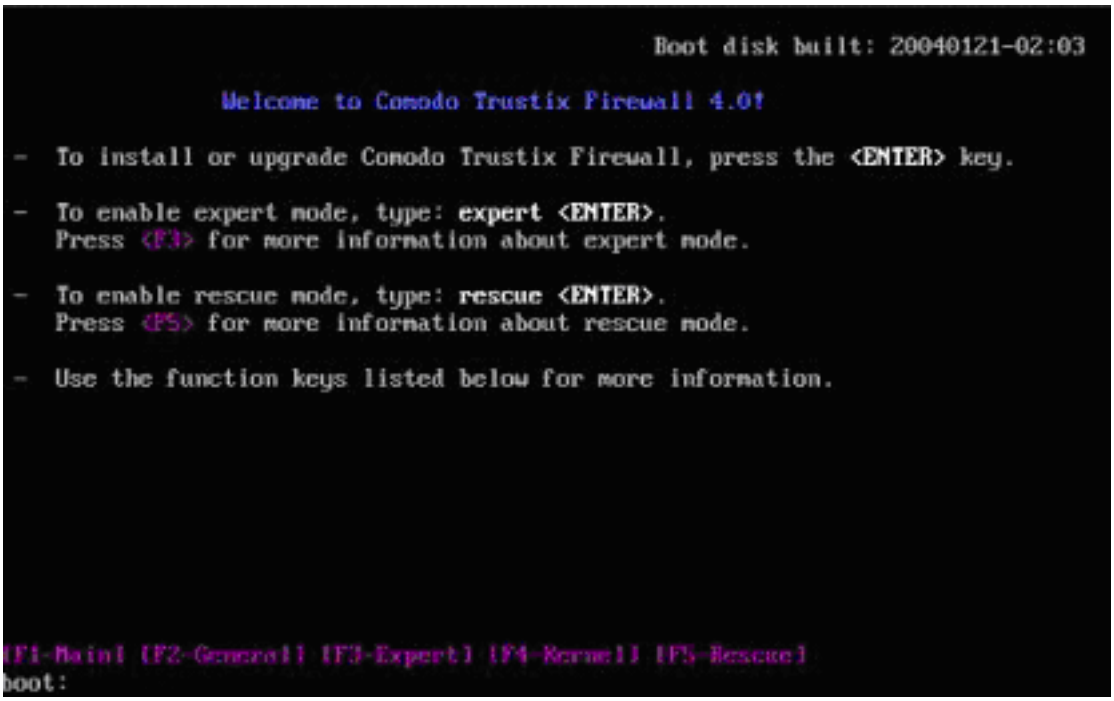
Hostname (domain name) for the Firewall.

Booting Up

Place the Firewall CD into the computer. Power the machine up. The installation process should automatically start.

[If the installation does not start, change the BIOS settings on the machine to boot from the CD-ROM drive.]

You should see the following screen upon starting up**.**


Boot disk built: 20040121-02:03
Welcome to Comodo Trustix Firewall 4.0!
- To install or upgrade Comodo Trustix Firewall, press the <ENTER> key.
- To enable expert mode, type: expert <ENTER>.
Press <F3> for more information about expert mode.
- To enable rescue mode, type: rescue <ENTER>.
Press <F5> for more information about rescue mode.
- Use the function keys listed below for more information.
[F1-Main] [F2-General] [F3-Expert] [F4-Kernel] [F5-Rescue]
boot:

Press the <ENTER> key to begin the installation.

Keyboard Setup

Now choose the keyboard layout/language for the firewall.

Patitioning the hard disk

The next step is partitioning the hard-disc. You should just select the 'Autopartition' option under most circumstances.

Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Disk Partitioning Setup
Automatic Partitioning sets up your partitioning based on your installation type. You also can customize the resulting partitions to meet your needs.
The manual disk partitioning tool, Disk Druid, allows you to set up your partitions in an interactive environment. You can set the filesystem types, mount points, size and more in this easy to use, powerful interface.
fdisk is the traditional, text-based partitioning tool. Although it is not as easy to use, there are cases where fdisk is preferred.
Autopartition
Disk Druid
fdisk
Back
<F1> for help ¦ <Tab> between elements ¦ <Space> selects ¦ <F12> next screen

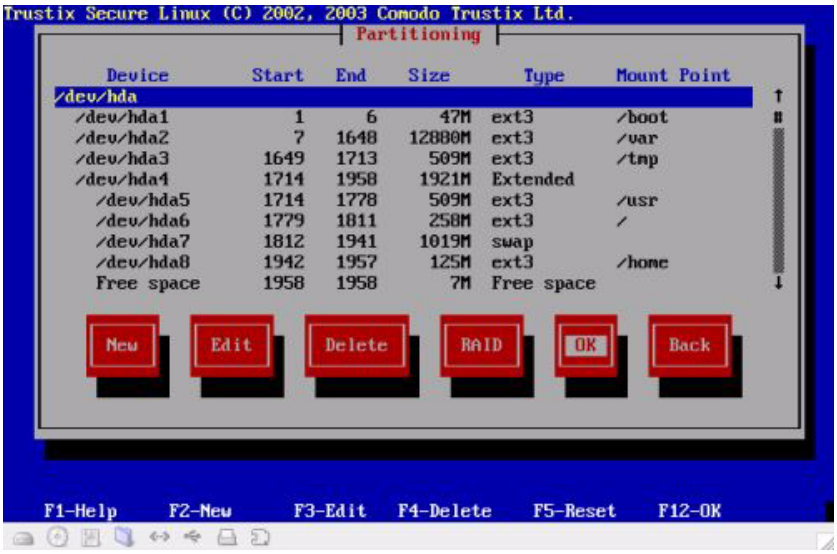
After selecting the 'autopartition' option you will be presented with options relating to the partitioning process and hard disk useage. Under usual circumstances, you will need to 'Remove all partitions on this system'. However, choose one of the other options should you require it.

You will be asked to confirm the hard-disc partition details.

Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Automatic Partitioning
Before automatic partitioning can be set up by the installation program, you must choose how to use the space on hard drives.
Remove all Linux Partitions on this system
Remove all partitions on this system
Keep all partitions and use existing free space
Which drive(s) do you want to use for this installation?
[*] hda
OK
Back
<F1> for help ¦ <Tab> between elements ¦ <Space> selects ¦ <F12> next screen

The installer will then show you the resulting partition layout of the drive.

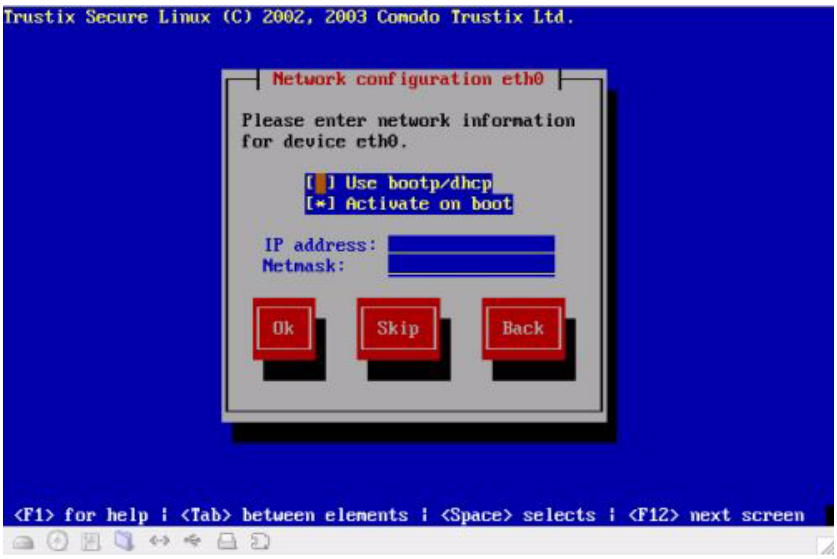
Select 'OK' once the settings are correct (see below/ next page).


Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Partitioning
Device Start End Size Type Mount Point
/dev/hda
/dev/hda1 1 6 47M ext3 /boot
/dev/hda2 7 1648 12880M ext3 /var
/dev/hda3 1649 1713 509M ext3 /tmp
/dev/hda4 1714 1958 1921M Extended
/dev/hda5 1714 1778 509M ext3 /usr
/dev/hda6 1779 1811 258M ext3 /
/dev/hda7 1812 1941 1019M swap
/dev/hda8 1942 1957 125M ext3 /home
Free space 1958 1958 7M Free space
New
Edit
Delete
RAID
OK
Back
F1-Help F2-New F3-Edit F4-Delete F5-Reset F12-OK

Network Settings

The installer will then ask for the network settings for each network card you have on the system. (You should have one network card for each zone on the firewall).

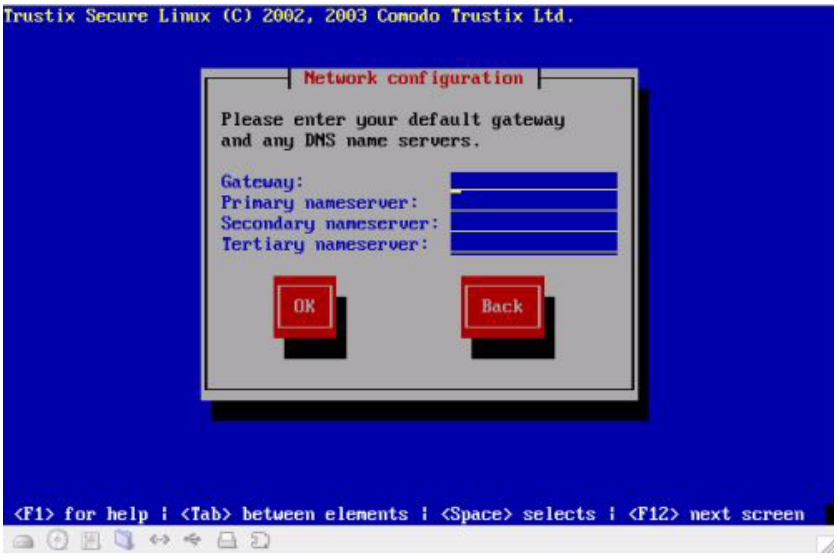
In this section you need to specify the IP address and Subnet Mask.



[Repeat as necessary for each network card.]

Now you will need to enter the default gateway and nameserver settings.

You will need to enter the IP address of at least 1 nameserver, though not all 3 are required.



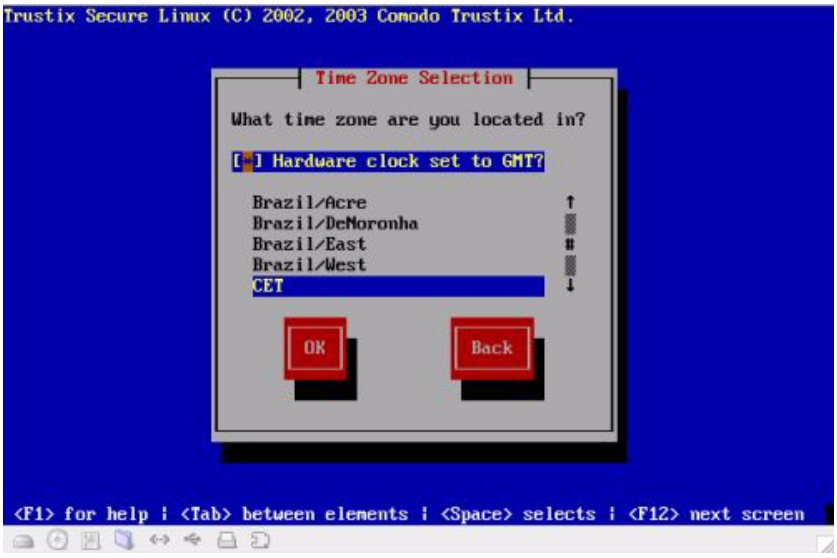
Host Configuration

Now you need to enter the hostname for the firewall.

If you have no hostname set up for the firewall, you can simply enter the IP address of the external (internet) network card.

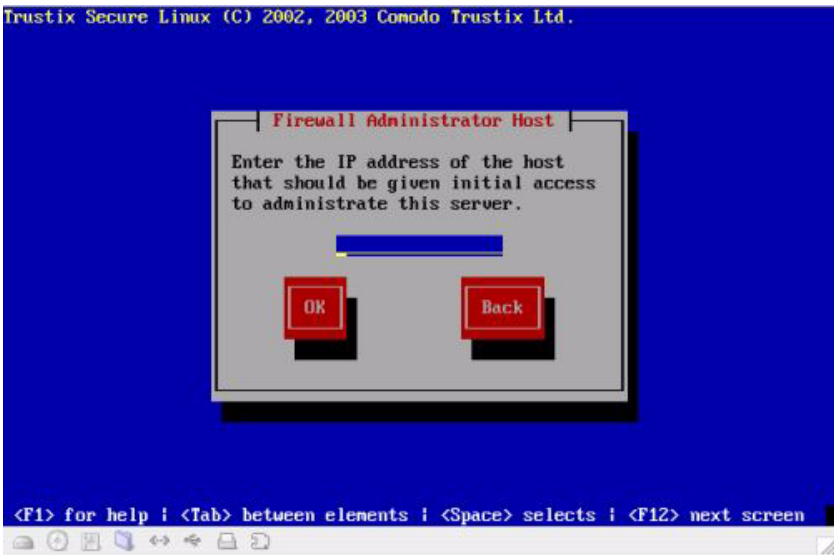
Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Hostname Configuration
The hostname is the name of your computer. If your computer is attached to a network, this may be assigned by your network administrator.
The hostname should be a fully qualified domain name.
Example: myhost.mydomain.topleveldomain
Hostname
OK
Back
<F1> for help ¦ <Tab> between elements ¦ <Space> selects ¦ <F12> next screen

Choose the time zone the server is located in.



Remote Configuration

Finally, you need to specify the IP address of the machine you will first use to administer the firewall remotely from.


Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Firewall Administrator Host
Enter the IP address of the host
that should be given initial access
to administrate this server.
OK
Back
<F1> for help ¦ <Tab> between elements ¦ <Space> selects ¦ <F12> next screen

The firewall will now begin to format and partition the hard disk, and install the software.

This will take from 10-20 minutes, depending on the speed of the hardware and size of the hard drive.

Once completed, you should press <enter> at the confirmation screen, and the system will eject the CD and reboot the machine into the firewall interface.

Finalising the installation

This final installation stage requires you to configure some simple settings on the firewall itself. Once this is completed, you can then remotely configure the firewall from a remote computer.

The firewall will require a password to access the interface.

The default password is 'trustix'.

This can (and should!!) be changed later via the interface. [See the full User Guide for details on changing this].

Within the interface, choose the 'Configure Networks' option

For each network card, you will need to name the Zone. Choose the network card, press enter, move down to the 'Zone' setting, and enter a name [e.g. LAN, Internet, DMZ etc.]

Once you have completed Configuring the networks, choose the 'Set Default Gateway'.

The default gateway will already be entered. You need to choose which network interface that the gateway is accessible from.
(note It is a good idea at this point to double check at that the default gateway is correct)

Finally, you need to choose the menu item 'Set LAN Interface'.

Select the network interface that the LAN is connected to.

The firewall is now set up and ready to licensed.

Part 2: Licensing

This guide will help you to install, license and set up basic rules on your Trustix Enterprise Firewall.

Checklist:

Trustix Enterprise Firewall, installed and configured as per Part 1 of this guide.

Client Configuration

Locate the machine with the IP address that you specified in the Remote Configuration section of Part 1 of this guide.

Insert the Firewall CD into the CD-ROM drive, and (under Windows) the Firewall XSentry Client should begin the installation automatically.

Once installed, launch the Client program.

The Client should then prompt you with a login box as below:

Enter the IP address of the Firewall, the username and the password

NOTE

The firewall installation procedure has **ALREADY** set the username and password up automatically.

The **default** Username/Password **MUST** be used in order to login in to the firewall.

USERNAME: **admin**

PASSWORD: trustix

This is the initial, default, combination. Trustix encourages you to alter the password after the client installation process has been completed. Choose a password that is secure and known only to users who you wish to have administrative access to the firewall.

The client will then login to the Firewall.

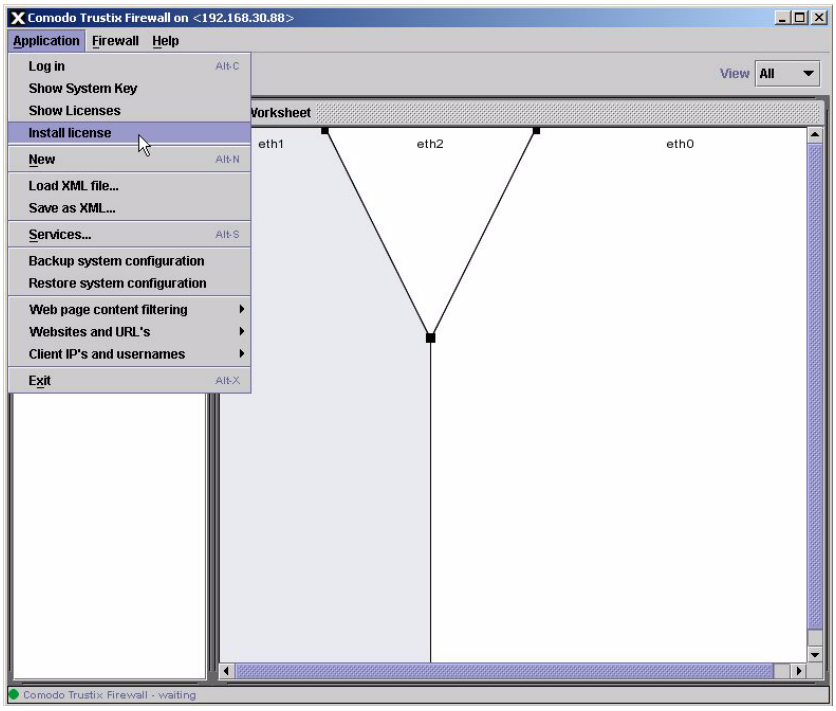
Installing the License

The Firewall will then inform you that there are no correct licenses on the Firewall. Click OK when the window pops up.

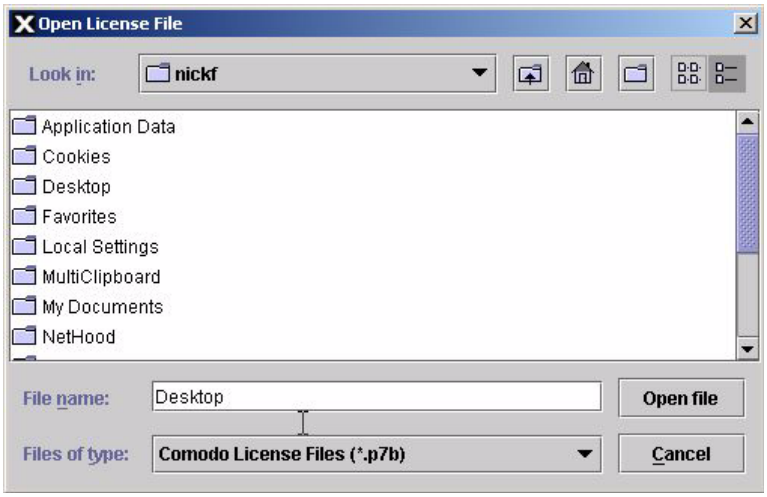
The Firewall will then show you a box containing the 'System Key'. Click OK to close this window also.

Save the license file you have received via email to your computers hard-drive.

Go to the 'Application' menu, and choose the option 'Install License'.



In the window that appears, change the 'File Type' to 'Comodo License Files (*.p7b)'



Locate the license file on your computer.

Click 'Open'.

The license file should then install, and the Firewall is ready to use.

What’s new in Trustix Enterprise Firewall 4.6

New features incorporated into Trustix Enterprise Firewall 4.6 include:

CORBA Replaces XSentry Code

The XSentryd daemon is now standalone as the XPloyd daemon has been removed from the Firewall Server. The communication between the Java client GUI and the Firewall Server is now through a powerful lightweight protocol that replaces CORBA and this communication is secured through JSSE (Java Secure Socket Extention) and stunnel.

DHCP Server and Relay support

DHCP (Dynamic Host Configuration Protocol) is a protocol that allows network administrators centrally manage and automate the assignment of dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

DHCP is built on a Client-Server model and relay. If DHCP Server is running on other subnet then, we can configure DHCP relay to forward request. In other words, using relay we can use other subnet DHCP server.

Monitoring and Alerts

To provide overall security a Firewall is required. But, it is equally important to regularly monitor its logs and current activities. It is also important to maintain alerts for important activities.

This module provides an excellent means to examine what's hitting your server and fix problems before they get out of hand.

Monitoring

Monitoring offers the current information about Firewall Server. They include:

- Network Configuration Information
  - List of all the devices of the firewall server
  - Status of all devices (Active / Inactive)
  - IP Address and Zone information of each device.
- Services Available
  - Service name
  - Status (Running / stopped)
- Remote Login
  - IP Address
  - User Name
  - Date-Time
- Port Status
  - Port number
  - Description
  - Port state
- Disk Information
  - Mount Point
  - File System Used
  - Capacity
- Important Latest Log

Alerts

A default alerts configuration file is present in the firewall. You can add/delete/edit alert configuration.

The following four types of alerts are available in the firewall:

- Admin Events
- Server Events
- Hardware Events
- Network Events

You can also add the following five types of alerts in the Firewall:

- Warning
- Email
- Beep
- Run program

Network Configuration

Configuration of network devices has become a critical requirement for administrators in today's highly inter-operable networks. Main objective of this module is to provide flexibility to the administrator for configuring the network. This module provides more important features like activating/deactivating the network device, setting the LAN and gateway interface, adding/removing/editing hosts from /etc/hosts file.

ARP Proxy

Proxy ARP (RFC 1027) is a way to make a machine physically located on one network appear to be logically part of a different physical network connected to the same router/firewall. Typically, it allows you to hide a machine with a public IP address on a private network behind a router, and still have the machine appear to be on the public network "in front of" the router. The router "proxys" ARP requests and all network traffic to and from the hidden machine to make this fiction possible.

Advanced Logging

Advanced Logging helps in keeping track of possible access problems, provides data on the effectiveness of your rule sets, and documents hack attempts. Advanced Logging helps you to store this type of attempts in a database or file, and access this information in a fine manner. Monitoring such activity provides an excellent means to check out what's hitting your server and fix problems before they get out of hand.

Static Routing

Static route entries can be added/removed from the Java client GUI.

Firewall policies within a subnet

You can add entities and set rule inside the subnet from Java client GUI.

Xsadm console menu option from Java GUI

All the ‘xsadm console’ menu options are now available from the Java client GUI.

User Management

The ‘xsadm console’ and Java client GUI contain the follow features:

- Add user
- Delete user
- Change password
- Assign one or more IP address to user

High Availability Modifications

You can configure High Availability using Java client GUI. A high availability backup feature is added in this version, which takes care of updating the important configuration files from the master machine to the slave machine. The user can edit the /opt/xsentry/etc/habackup.cfg file to specify the required configuration files that are to be backed up.

What’s new in Trustix Enterprise Firewall 4.1

New features incorporated into Trustix Enterprise Firewall 4.1 include:

Traffic Shaping

Easy to use traffic shaping with hi/medium/lo prioritising for each rule present in the gui. Effective traffic shaping settings can optimise internet bandwidth distribution throughout a network, thus avoiding bottlenecks and increasing network speed and stability.

Virtual LAN Support

The administrators can use an interface of the firewall in VLAN 'trunk mode' VLANs will be treated as exactly the same thing as a physical interface for all rule setting and entity creation (the VLANs are shown as zones in the gui). Virtual LANs can now be created modified and removed from both the server side (xsadm console) and the client side (XSentry console)

High Availability Modifications

Altered the high availability option from a 'master-slave' relationship to a 'master-master' relationship. In the event of hardware or software failure, the backup server will now seamlessly assume control of firewalling duties and will continue to do so even after the original machine has been restored to full functionality. The original machine then becomes the backup

What's new in Trustix Enterprise Firewall 4.0

New features available in the Trustix Firewall 4.0 include:

- Upgraded Linux kernel on server to 2.4.21.
- Stateful packet inspection (connection tracking).
- Source network address translation (NAT). This changes the source address of connections to something different, hiding the real address. Masquerading is a special case of source NAT.
- Destination network address and port translation (NAPT). Port forwarding is a special case of destination NAPT.
- MAC filtering. An IP address can be bound to a specific MAC address. Packets not satisfying the IP address/MAC address binding will be rejected by the firewall.
- Upgraded FreeS/WAN to version 2.0.
- Opportunistic encryption.
- Improved user interface dialogs.

Netfilter and Iptables

Netfilter/iptables is the firewalling subsystem in the Linux 2.4 kernel. It is a flexible and extensible infrastructure for packet routing and filtering. It provides stateful packet filtering, all kinds of NAT (Network Address Translation) and other advanced packet processing.

What is new in Trustix Enterprise Firewall 3.5

The Trustix Firewall 3.5 includes a whole new set of features, specifically designed to meet the requirements of large enterprise customers. Version 3.5 is separated into 3 product categories; Small Office, Professional and Enterprise.

These 3 versions are all built on the same operating system kernel, server and client architecture and only separates the product in market positioning and message to market.

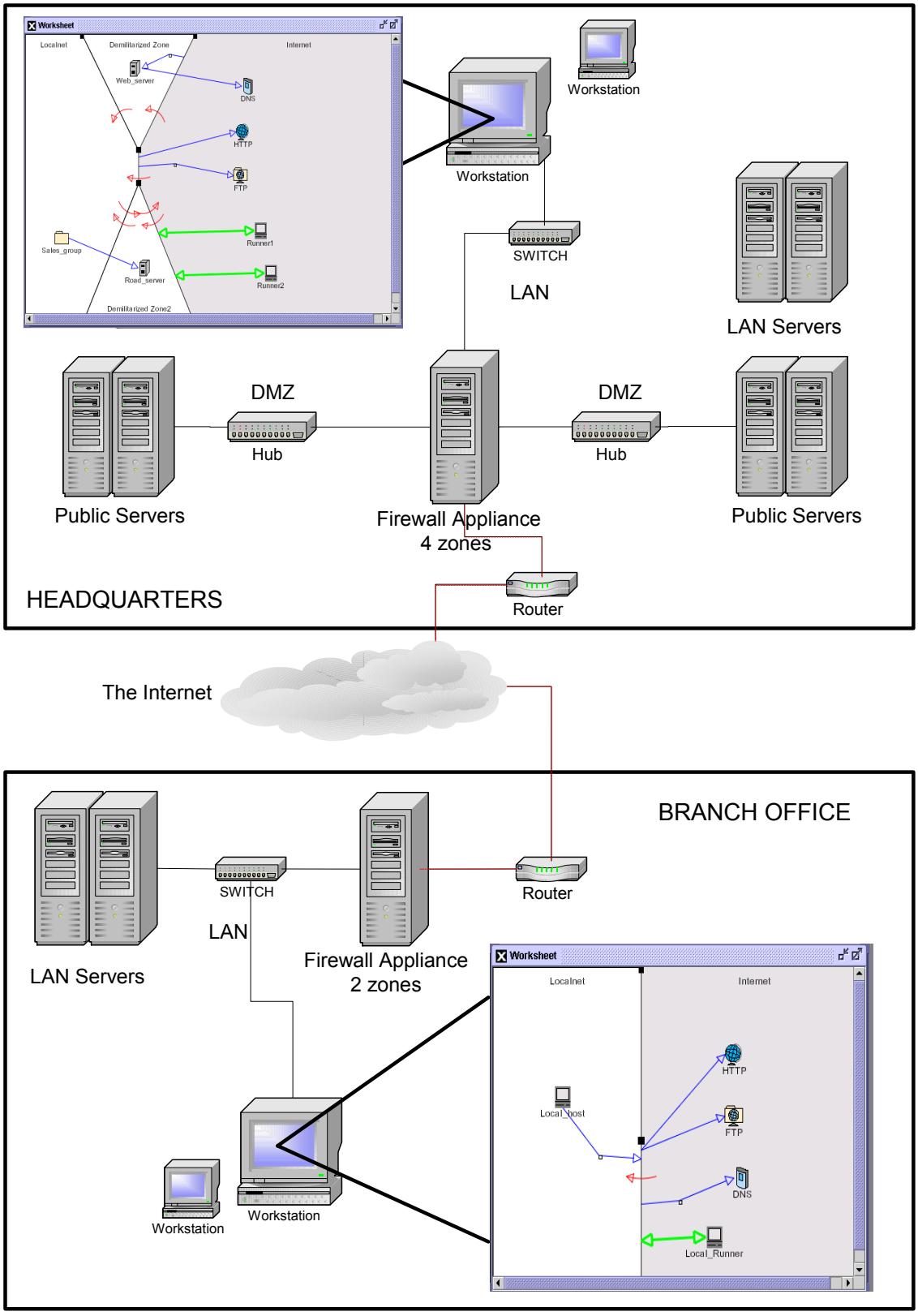
New features available in the Trustix Firewall 3.5 include:

- Upgraded Linux kernel on server to 2.2.25.
- Improved hardware support, specially for IBM eServer xSeries hardware.
- System monitoring, with e-mail notification, for various components of the system. The logging file system is monitored, and will trigger an e-mail alarm if the file system is more than 80% full.
- A high availability solution with a failover feature. Two firewalls in a master/slave configuration are used to minimize downtime due to hardware or software errors on the firewall servers.
- The high availability feature is a highly advanced feature, which requires a high degree of skill and knowledge about network topology and security. See “High Availability,” on page 135.
- A framework for traffic control and traffic shaping is included. This allows you to define your own traffic priorities based on port or protocol.
- A transparent proxy server will cache HTTP traffic passing through the firewall. This feature does not require end users to manually re-configure their web browsers.
- Administration of the firewall will be blocked after a predefined number of failed logins. This is to stop hackers with access to the administration client from guessing administrator usernames and passwords.

Firewall Overview

The Trustix Firewall consists of two modules, the *firewall* server and the *firewall administration client*. The server is a reliable, high performance Linux firewall, providing:

- Stateful packet filtering and connection tracking
- Virtual Private Networks (VPN) and road warrior support
- Source Network Address Translation (source NAT)
- Destination Network and Port Address Translation (destination NAPT).
- Support for 2 to 129 PCI network interface cards. (In most cases however, the practical hardware limit is 24 or less.)
- Logging
- Transparent proxy
- Fault-tolerance with failover in case of hardware or software failures
- Traffic control and traffic shaping
- The firewall client is the tool for administration of the firewall. It can be installed on any Windows or Linux computer on the local network. It allows administration of the firewall in a unique and intuitive graphical environment:
- Drag and drop graphical environment
- Remote and secure administration from the LAN or predefined locations on the Internet
- Administration of multiple firewalls from the same client
- Log analysis. With the log module you can retrieve and analyse logs.


Worksheet
Localnet
Demilitarized Zone
Internet
Web_server
DNS
HTTP
FTP
Runner1
Sales_group
Road_server
Runner2
Demilitarized Zone2
Workstation
Workstation
SWITCH
LAN
LAN Servers
DMZ
Hub
DMZ
Hub
Public Servers
Firewall Appliance
4 zones
Public Servers
HEADQUARTERS
Router
The Internet
BRANCH OFFICE
SWITCH
LAN
Router
LAN Servers
Firewall Appliance
2 zones
Workstation
Workstation
Worksheet
Localnet
Internet
HTTP
Local_host
FTP
DNS
Local_Runner

Conceptual model of The Firewall and client in an enterprise network.

About this User Guide

This guide assumes that the reader knows how to perform basic operating system tasks and is familiar with the fundamentals of computer networking. It is written both as a tutorial and as a reference. Most of the reference information can be found in the appendices. Please note that this user guide does not address the installation and configuration of the firewall hardware.

Conventions

Conventions used in this user guide:

- New terms and concepts are written in *italic*. *Italic* is also used for emphasis in running text.
- Menu items and buttons are written in **bold** text.
- Keys entered on the keyboard are enclosed in brackets, e.g. <ESC>
- Commands and file names are written in plain text.

Additional Resources

Online help and support resources are available on the World Wide Web. Please visit the Trustix web site for additional information and FAQ.

Trustix™

Chapter 3

Firewall Server Installation

Pre-installed Firewall Server

In most cases, your Trustix Firewall server has been pre-installed by your Trustix reseller. If so, you can ignore this chapter, and proceed to “First-time Configuration of Firewall” on page 41.

However, if you have bought the firewall as a software package, this chapter will tell you how to install the firewall server.

Prerequisites

Before installation of the Trustix Firewall server, collect the following information.

- The IP-addresses for the firewall on the LAN, the Internet and any DMZs or other zones.
- The mask and broadcast address for all networks.
- The IP address of the DNS server.
- Your Internet service provider’s gateway address. This is used as the firewall’s gateway address.
- The IP address(es) of the computer(s) where the client should be installed.

System Requirements

Firewall Server

The computer dedicated to be the firewall server must meet the following requirements:

Table 3-1 Server Requirements.

Element	Minimum	Recommended
CPU	Intel Pentium 90 Mhz	Intel Pentium III or better.
RAM	32 MB	128 - 256MB
CD-ROM Drive	Any Speed	Any Speed
Network card	2 PCI network Interface cards	4 PCI network Interface cards
Hard drive free space	600 MB	9 GB

System Performance Considerations

When deciding what hardware to include in the firewall, the following should be considered.

- CPU
  Although the Trustix Firewall server has a moderate CPU requirement, it should be understood that CPU speed affect firewall throughput. It should also be noted that VPN requires significantly needs more CPU power than ordinary routing.
- Memory
  The amount of memory determines the number of concurrent connections the firewall can handle. Memory size also has an impact on performance. A firewall with one or several VPN connections will require more memory.
- Disk space
  The log functionality can generate large files. Make sure enough hard disk space is provided to serve the organization's network logging policy. A SCSI disk is preferred if you have demanding logging requirements.
- Network devices
  ISA cards are not supported by the Trustix Firewall server.

Firewall Client

Supported Operating Systems:

Microsoft Windows 98/ME/NT/2000/XP and most Linux distributions are supported.

The computer(s) that will run the administration client must meet the following requirements:

Table 3-1 Client Requirements.

Element	Minimum	Recommended
CPU	Intel Pentium II or better.	Intel Pentium II, III or better.
RAM	64MB	128 MB or more
CD-ROM Drive	Any Speed	Any Speed
Pointing device	Any mouse with two or more buttons.	Any mouse with two or more buttons.
Hard drive free space	50 MB	50 MB

Firewall Server Installation

Preparation

Make sure that all network interface cards are properly installed. Do not connect the firewall computer to any network before installing the software.

Installation

This guide will help you to install, license and set up basic rules on your Trustix Firewall.

Checklist:

PC-compatible computer for the firewall.

Trustix Enterprise Firewall CD

License certificate for the Firewall

IP address settings for your network:

Gateway IP address

Nameserver IP addresses

IP address settings for each network card (zone)

IP address of the administrator's machine

Hostname (domain name) for the Firewall.

Booting Up

Place the Firewall CD into the computer. Power the machine up. The installation process should automatically start.

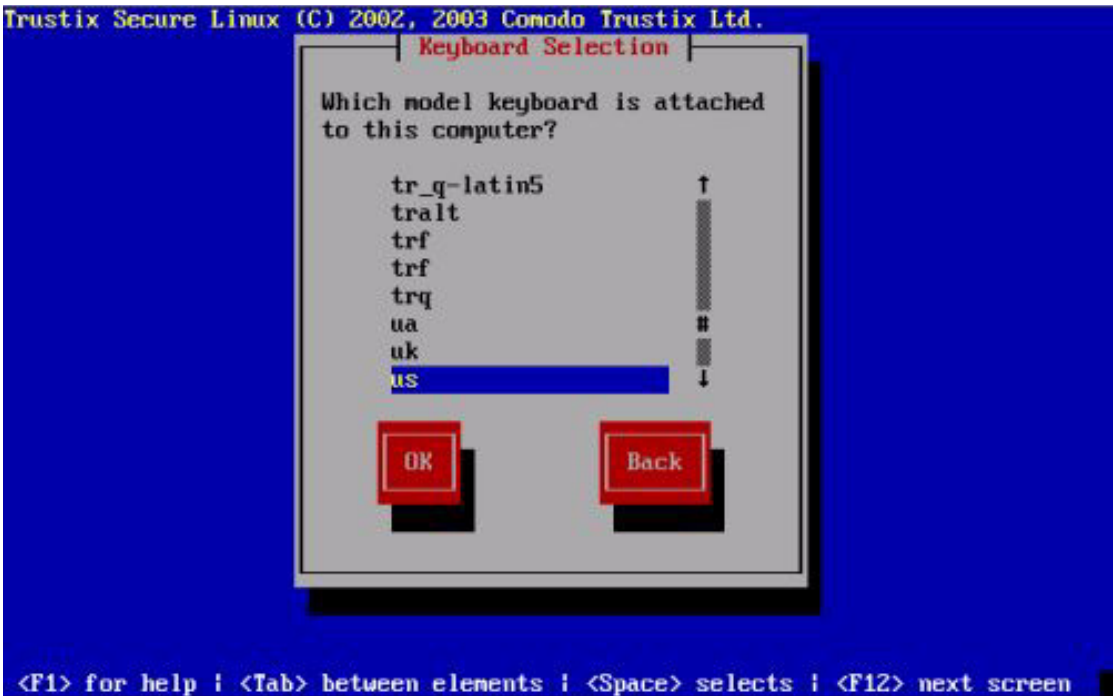
[If the installation does not start, change the BIOS settings on the machine to boot from the CD-ROM drive.]

You should see the following screen upon starting up

Press the <ENTER> key to begin the installation.

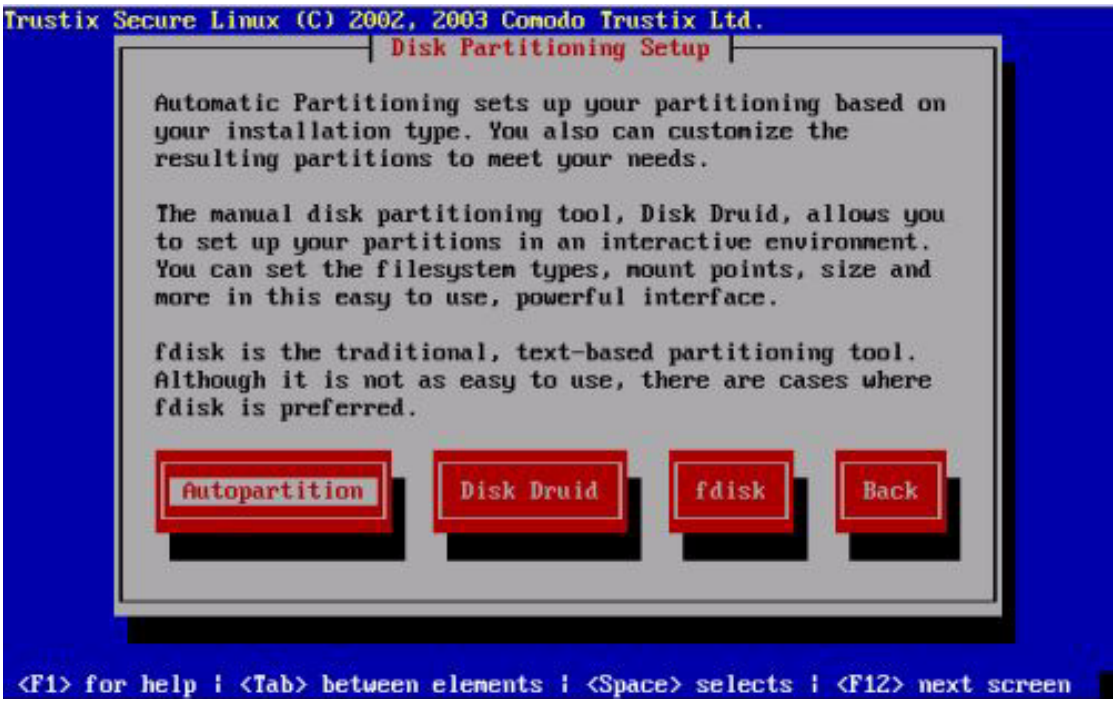
Keyboard Setup

Now choose the keyboard layout/language for the firewall.



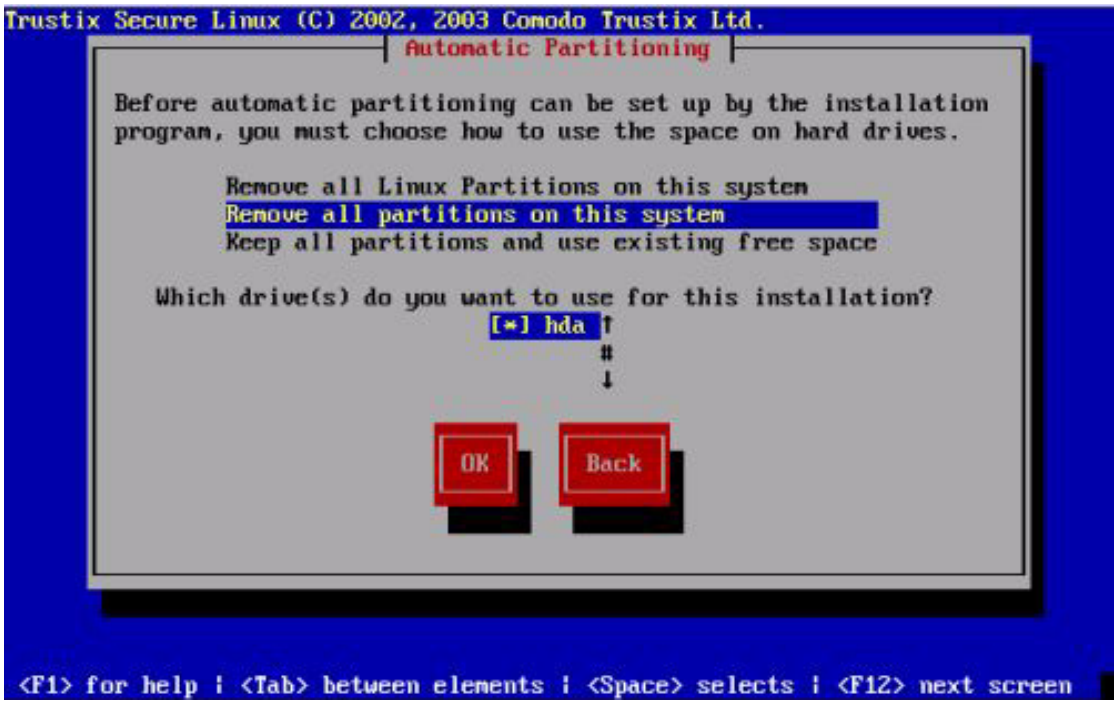
Patitioning the hard disk

The next step is partitioning the hard-disc. You should just select the ‘Autopartition’ option under most circumstances.


Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Disk Partitioning Setup
Automatic Partitioning sets up your partitioning based on your installation type. You also can customize the resulting partitions to meet your needs.
The manual disk partitioning tool, Disk Druid, allows you to set up your partitions in an interactive environment. You can set the filesystem types, mount points, size and more in this easy to use, powerful interface.
fdisk is the traditional, text-based partitioning tool. Although it is not as easy to use, there are cases where fdisk is preferred.
Autopartition
Disk Druid
fdisk
Back
<F1> for help ¦ <Tab> between elements ¦ <Space> selects ¦ <F12> next screen

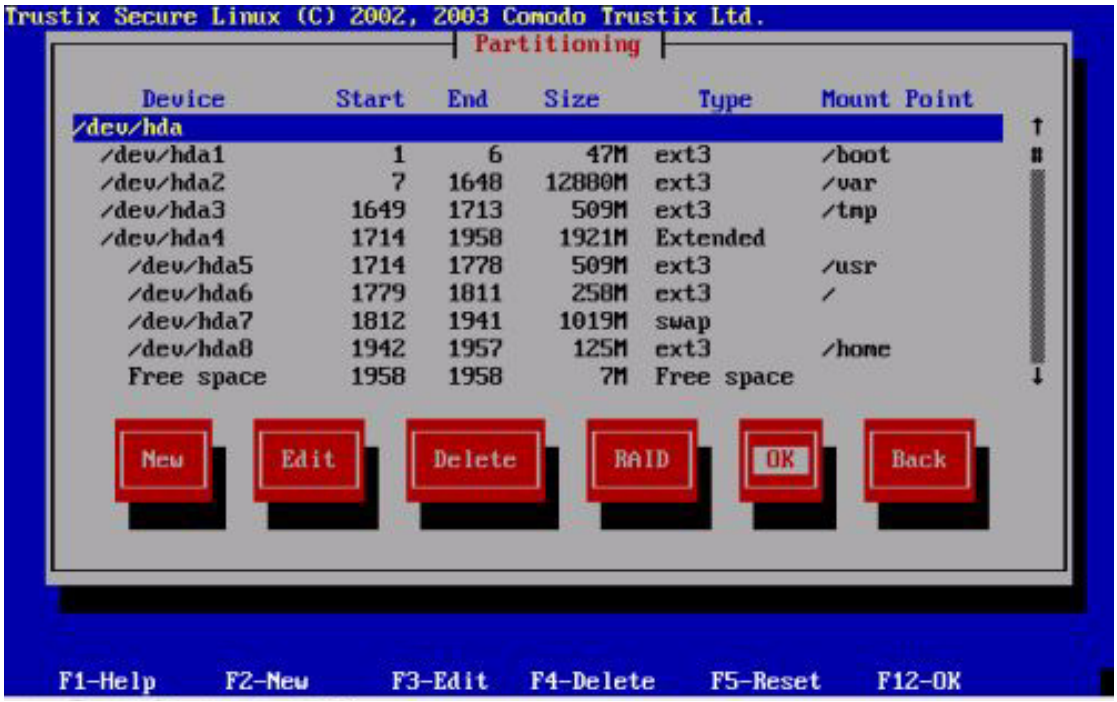
After selecting the ‘autopartition’ option you will be presented with options relating to the partitioning process and hard disk useage. Under usual circumstances, you will need to ‘Remove all partitions on this system’. However, choose one of the other options should you require it.

You will be asked to confirm the hard-disc partition details.


Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Automatic Partitioning
Before automatic partitioning can be set up by the installation program, you must choose how to use the space on hard drives.
Remove all Linux Partitions on this system
Remove all partitions on this system
Keep all partitions and use existing free space
Which drive(s) do you want to use for this installation?
[*] hda
OK
Back
<F1> for help ¦ <Tab> between elements ¦ <Space> selects ¦ <F12> next screen

The installer will then show you the resulting partition layout of the drive.

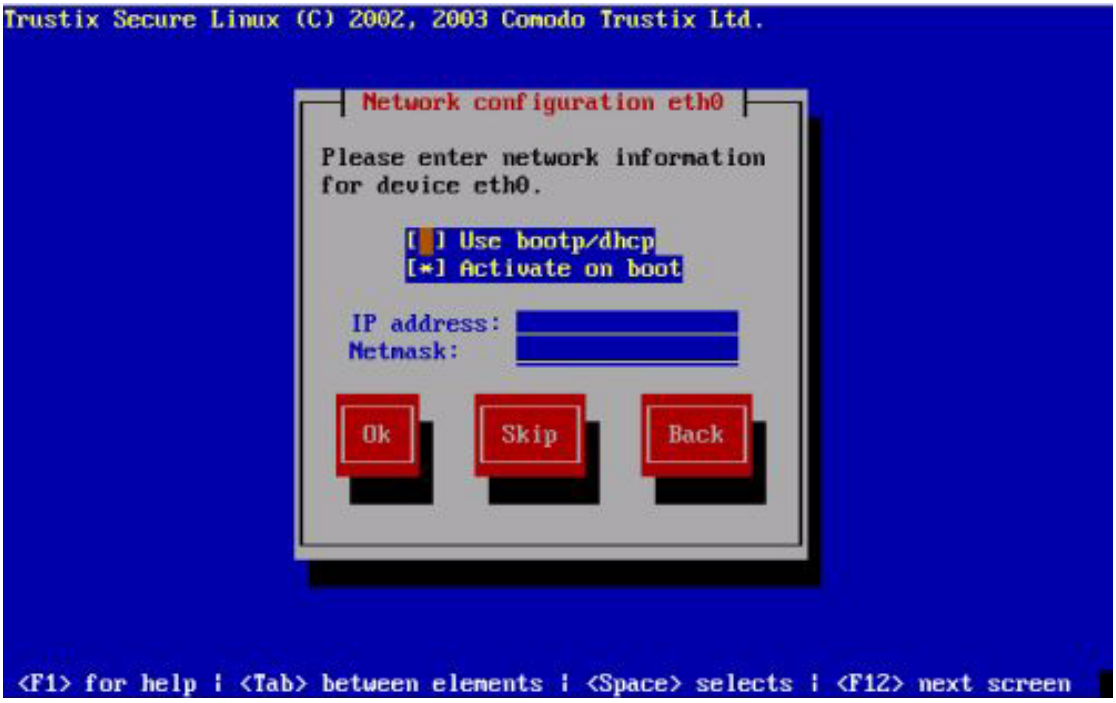
Select 'OK' once the settings are correct (see below/ next page).


Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Partitioning
Device Start End Size Type Mount Point
/dev/hda
/dev/hda1 1 6 47M ext3 /boot
/dev/hda2 7 1648 12880M ext3 /var
/dev/hda3 1649 1713 509M ext3 /tmp
/dev/hda4 1714 1958 1921M Extended
/dev/hda5 1714 1778 509M ext3 /usr
/dev/hda6 1779 1811 258M ext3 /
/dev/hda7 1812 1941 1019M swap
/dev/hda8 1942 1957 125M ext3 /home
Free space 1958 1958 7M Free space
New
Edit
Delete
RAID
OK
Back
F1-Help F2-New F3-Edit F4-Delete F5-Reset F12-OK

Network Settings

The installer will then ask for the network settings for each network card you have on the system. (You should have one network card for each zone on the firewall).

In this section you need to specify the IP address and Subnet Mask.



[Repeat as necessary for each network card.]

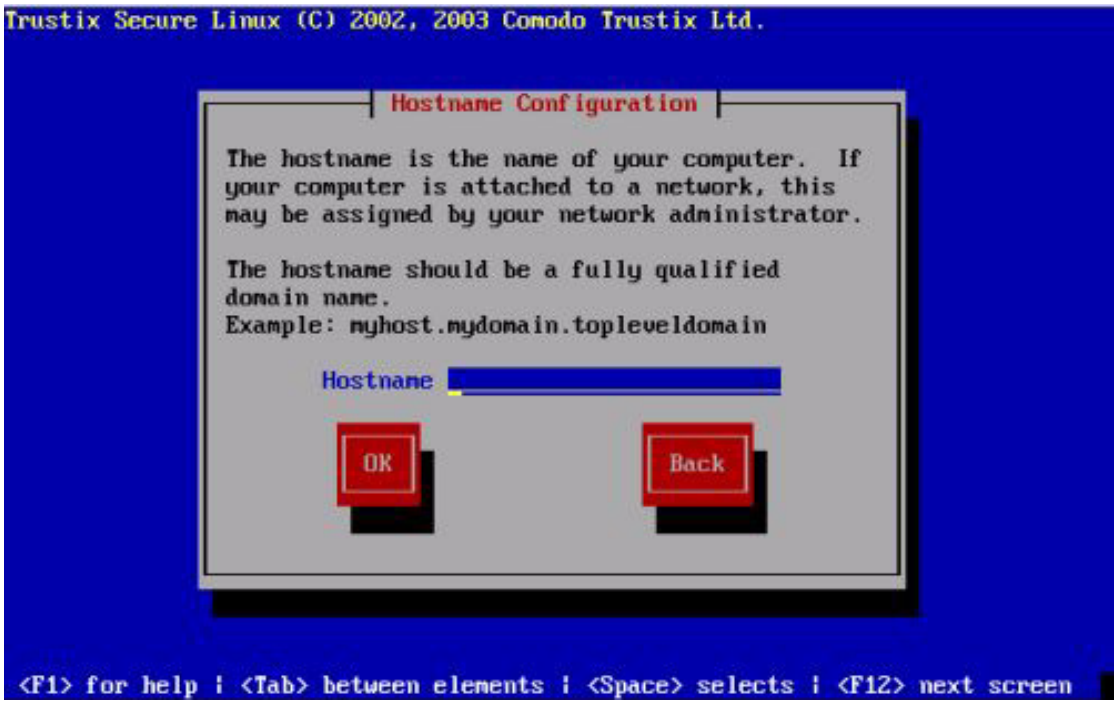
Now you will need to enter the default gateway and nameserver settings.

You will need to enter the IP address of at least 1 nameserver, though not all 3 are required.

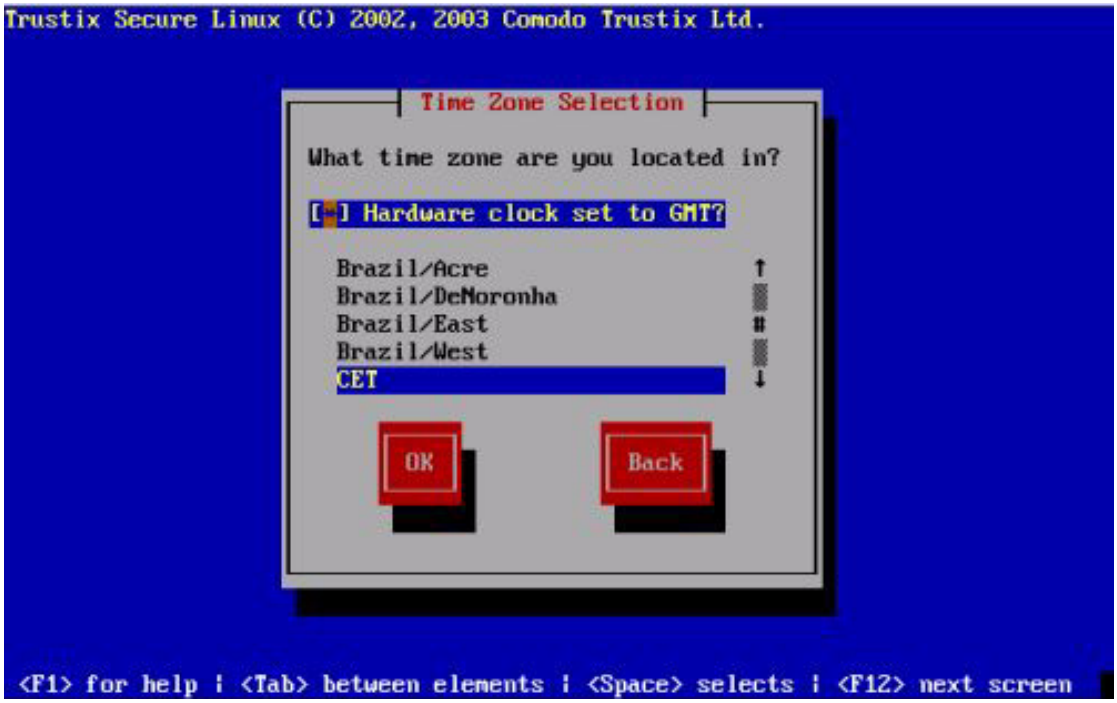
Host Configuration

Now you need to enter the hostname for the firewall.

If you have no hostname set up for the firewall, you can simply enter the IP address of the external (internet) network card.


Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Hostname Configuration
The hostname is the name of your computer. If your computer is attached to a network, this may be assigned by your network administrator.
The hostname should be a fully qualified domain name.
Example: myhost.mydomain.topleveldomain
Hostname
OK
Back
<F1> for help ¦ <Tab> between elements ¦ <Space> selects ¦ <F12> next screen

Choose the time zone the server is located in.



Remote Configuration

Finally, you need to specify the IP address of the machine you will first use to administer the firewall remotely from.

Trustix Secure Linux (C) 2002, 2003 Comodo Trustix Ltd.
Firewall Administrator Host
Enter the IP address of the host that should be given initial access to administrate this server.
OK
Back
<F1> for help ¦ <Tab> between elements ¦ <Space> selects ¦ <F12> next screen

The firewall will now begin to format and partition the hard disk, and install the software.

This will take from 10-20 minutes, depending on the speed of the hardware and size of the hard drive.

Once completed, you should press <enter> at the confirmation screen, and the system will eject the CD and reboot the machine into the firewall interface.

Finalising the installation

This final installation stage requires you to configure some simple settings on the firewall itself. Once this is completed, you can then remotely configure the firewall from a remote computer.

Trustix™

Chapter 4

First-time Configuration of Firewall

Before the Firewall can be used, information about the network infrastructure must be collected. To be able to use the firewall at all, you have to configure it with the following options in mind:

- The IP of the LAN interface
- The zone names
- The default gateway device
- Users allowed to use the Firewall
- Unblock traffic
- Enable license negotiating

This is done on the firewall console. The Firewall's console is a menu-based application that is always running.

Console Configuration

If you have purchased a Firewall, you will have to read the next section, to understand how to connect to the firewall server through a terminal interface.

> ***Note:*** *Naturally, you may simply connect a screen and a keyboard to your Firewall to perform the necessary configuration.*

Firewall Console

In some versions of the firewall, the user would like to configure the firewall server through a terminal or a laptop with a null-modem cable. This way of communicating with appliances is often seen on routers and switches.

1. Connect your laptop (or any other PC-compatible computer) to the firewall server's serial interface with a null modem cable. This cable is often referred to as "lap-link"-cable and is readily available in most computer stores.

   The serial interface on your firewall is known in Microsoft Windows as 'com1' and in Linux as 'ttyS0' or 'cua0' and is the first serial port on your computer.

   When your laptop is connected, you have to start a terminal application. To make it easier for you, we have included an application called "Tera Term" on the application-CD, which is a Microsoft Windows-based terminal application. Tera Term is loaded at the same time as the client applications into a folder at this location:

   <drive>:\Program Files\Comodo Trustix\Firewall 4\thirdparty\TeraTerm

   We have experienced problems when using the included Hyperterminal application in Microsoft Windows, and it is therefore recommended that you use the included “Tera Term” application from the firewall client CD-ROM

2. Make sure Tera Term is installed on your client computer (the laptop) and start it (either from the start-menu or from the Windows Explorer).

3. When your Tera Term application starts up for the first time, you are presented with a dialog asking for TCP/IP connection or Serial connection. Select the serial connection and leave port on “COM1”. Click **OK** and you are connected.

   If you would like to connect to the firewall from Tera Term again, use the **File-> New Connection** menu and use the COM1 port again.

   If you are not presented with the firewall console, you have no connection to the firewall and a blank screen will appear. This probably means that you have no cable connected between your laptop and firewall, or your cable is broken.

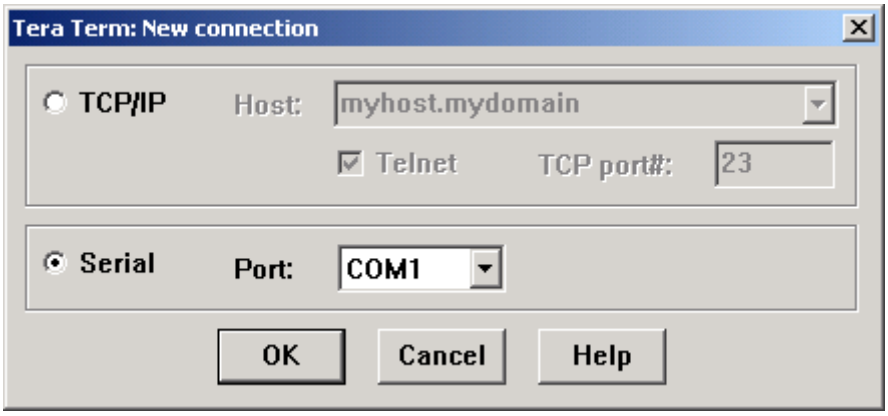


Figure 4-1 Tera Term, new connection.

Once connected, you have the same interface as if you were using a monitor and keyboard and you can proceed to the next section.

One good idea is to increase the transfer rate of the communication port (com1) to 115000 baud. This is done through the menu **Setup->Serial port** from within Tera Term (Figure 4-2).

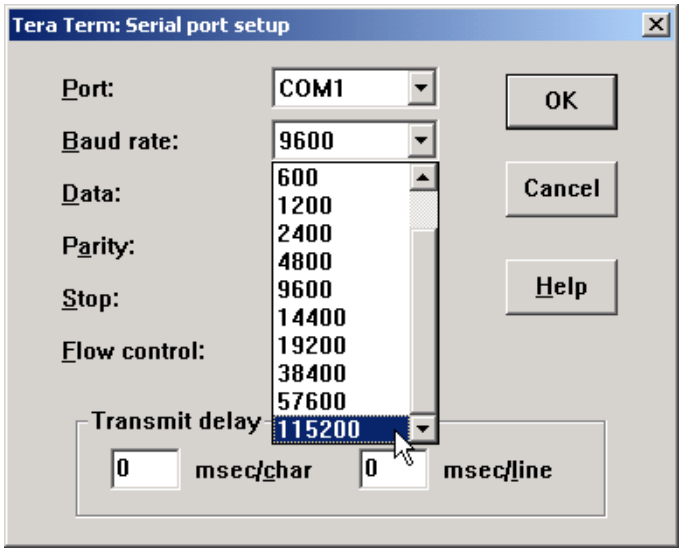


Figure 4-2 Tera Term, transfer rate.

For Linux-users, you can use the 'minicom'-application included in most Linux distributions. The same physical cable is required (null-modem) and you must connect this to your Linux client and the Firewall.

To connect to your Firewall after the initial configuration, you can either use the same procedure as described in this chapter, or you can use an ssh client to connect from your administrator PC.

Configuring the Firewall Console

Please acquire all information needed before starting the configuration process. See page 31.

Figure 4-3 Console login.

Logon to the firewall with the password set during installation. The scrollable menu shown in Figure 4-4 appears. Select **Configure networks**.

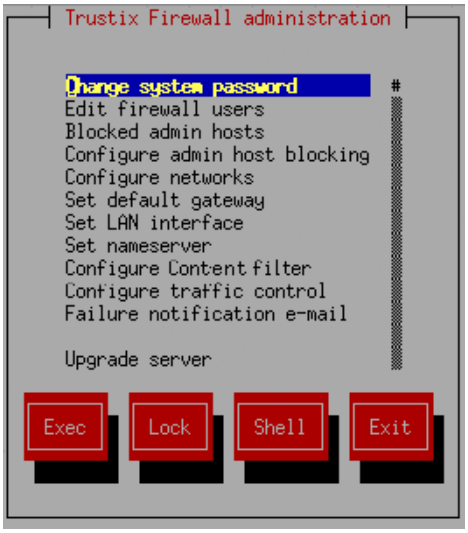


Figure 4-4 Console menu.

Setting the LAN Interface

Selecting **Set LAN interface** from the menu configures the LAN interface.
A list of network interface cards will be shown. Choose the network interface card that should belong to the LAN. One interface will not appear in the list. This is the interface that has been marked as the default gateway device.

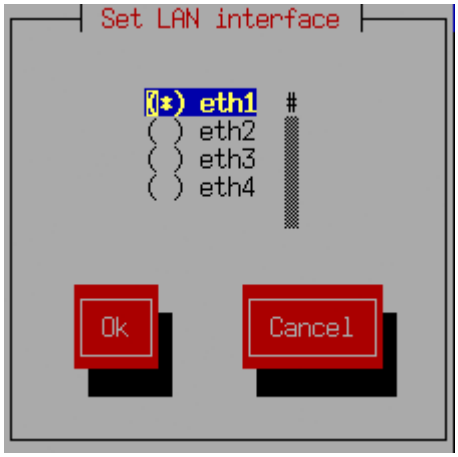


Figure 4-5 LAN interface.

Setting the Zone Names

The zones are configured by selecting **Configure networks** from the menu. A list of network devices will appear. The number of network devices should be the same as the number of network interface cards installed on the computer. The devices will be named `eth0, eth1, eth2` etc. These devices need to be assigned to zones.

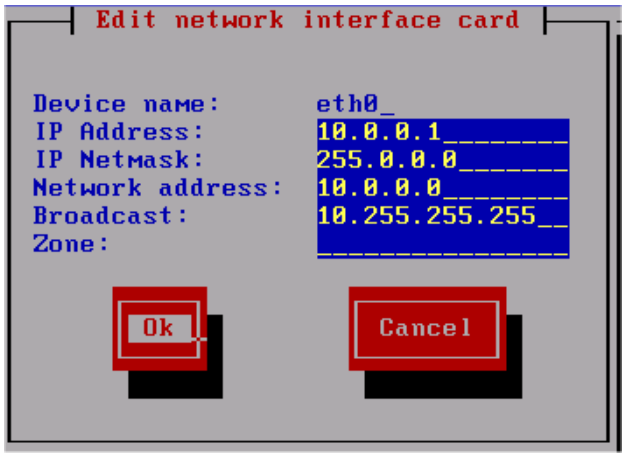


Figure 4-6 Network device configuration.

The information about IP Address, IP Netmask, Network address and broadcast were set during the first steps of installing the Firewall.

Enter the zones' names. Typically, `eth0` is named *Internet*, `eth1` is named *LAN* and the following zones are named *DMZ1, DMZ2* etc.

Setting Gateway

Selecting **Set default gateway** from the menu sets the gateway address.

The IP address used as the firewall's default gateway should be entered here, be sure to connect it to the correct network interface card. The Internet service provider should provide this address.

> ***Note:*** *Trustix recommend that eth0 is used as the default Gateway/Internet interface. Using other devices as default Gateway/Internet interface may cause client/server communication problems.*

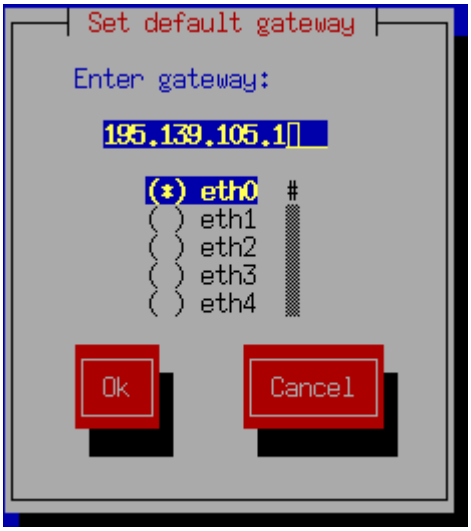


Figure 4-7 Gateway configuration.

Define Remote User

To use the unique graphical user interface of the Trustix Firewall client, you need to define a remote administrator that is allowed to manage the security policy of the firewall from an administration host. Select **Edit firewall users**, and enter the required information:

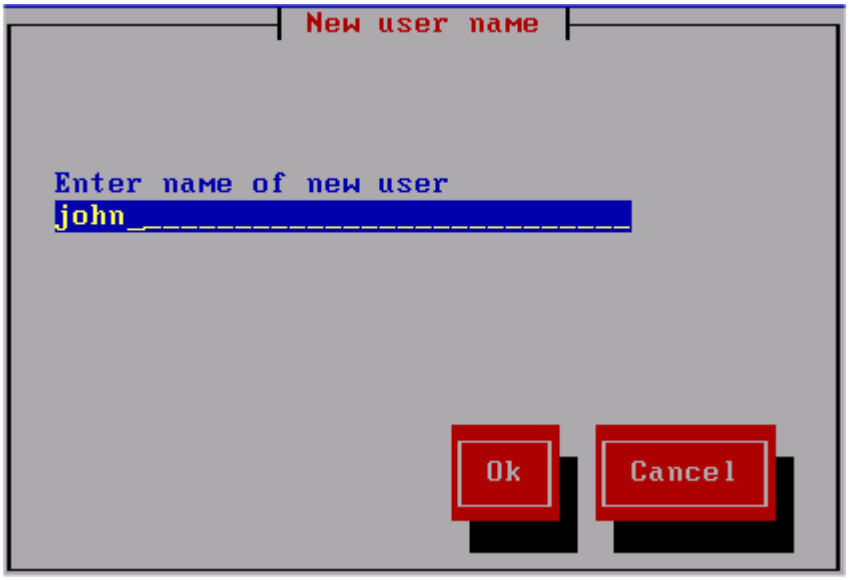


Figure 4-8 Add firewall user.

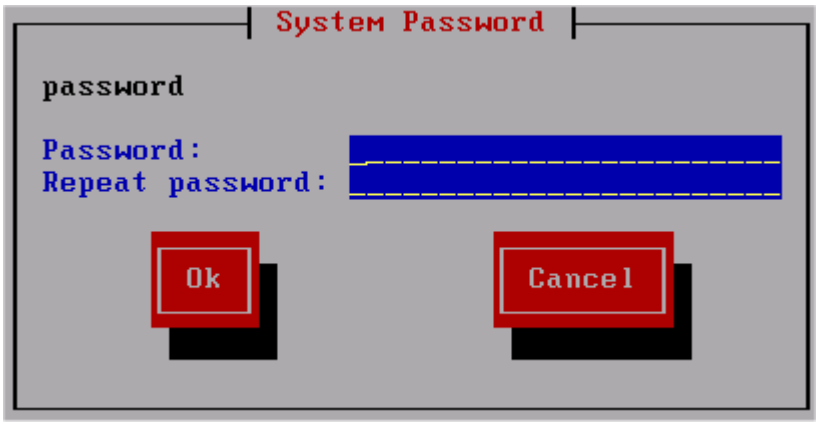


Figure 4-9 Enter password for firewall user.

Figure 4-10 The IP which the Firewall user can administrate the firewall from.

The IP addresses must be separated by commas. Use no blanks anywhere.

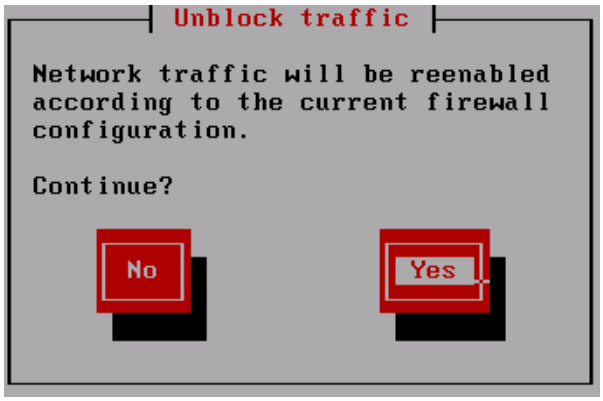


Figure 4-11 Unblock traffic.

Physical Installation

After configuring the network devices, they need to be connected to the correct networks. The firewall has two or more network interface cards installed. One should be linked to the LAN and the other to the connection to the Internet. The third/fourth (if installed) should be connected to the secure zone(s).

First, set the firewall server in test mode by selecting **Enable ping testing** from the main menu. In order to determine what network devices the networks should be connected to, *ping* is used. Ping is a program that sends packets to a computer in order to see if it's there. The Ping program comes with all Windows versions supported by the Firewall. Start by locating the LAN network device. After the LAN device has been found, repeat the procedure in order to locate the secure zone's network device(s). The last device is the Internet device. After locating all networks, disable ping testing on the firewall console.

Locating the LAN Network Device

1. Connect the cable to the LAN to the first network device on the firewall.
2. Open up a DOS Prompt window on a computer on the LAN, by selecting **MS-DOS Prompt** from the Start Menu.
3. Ping the firewall's LAN IP address, by giving the command `ping ip address`. E.g., `ping 10.0.0.1`. Remember, the firewall can only be pinged from the client workstation, and the firewall must be in ping-mode.
4. If the LAN is connected to the correct network device, the ping program will display replies from the firewall. The correct network device has been found.

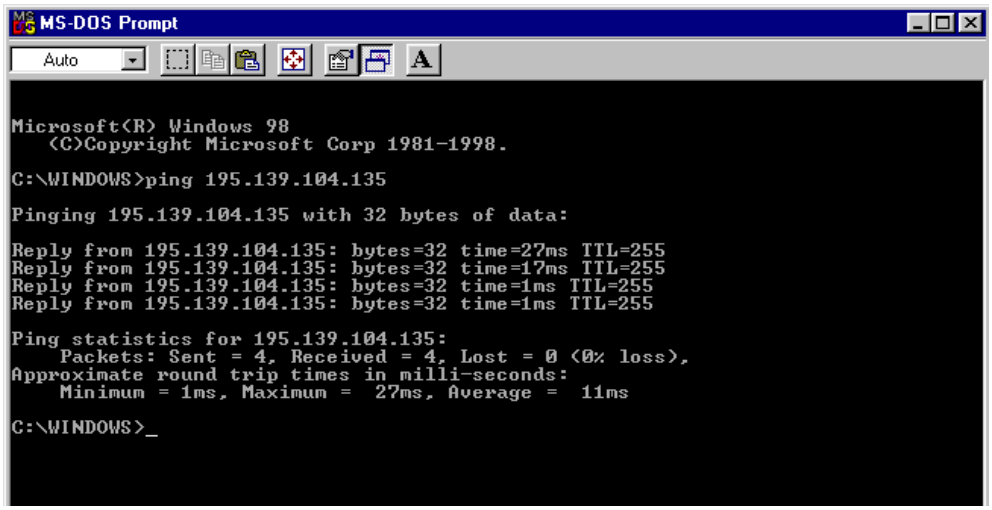

MS-DOS Prompt
Auto
Microsoft(R) Windows 98
(C)Copyright Microsoft Corp 1981-1998.
C:\WINDOWS>ping 195.139.104.135
Pinging 195.139.104.135 with 32 bytes of data:
Reply from 195.139.104.135: bytes=32 time=27ms TTL=255
Reply from 195.139.104.135: bytes=32 time=17ms TTL=255
Reply from 195.139.104.135: bytes=32 time=1ms TTL=255
Reply from 195.139.104.135: bytes=32 time=1ms TTL=255
Ping statistics for 195.139.104.135:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 27ms, Average = 11ms
C:\WINDOWS>_

Figure 4-12 Successful ping.

5. If the LAN is connected to a wrong network device, the ping program times out. If this is the case, move the network cable to the next network device, and try again.

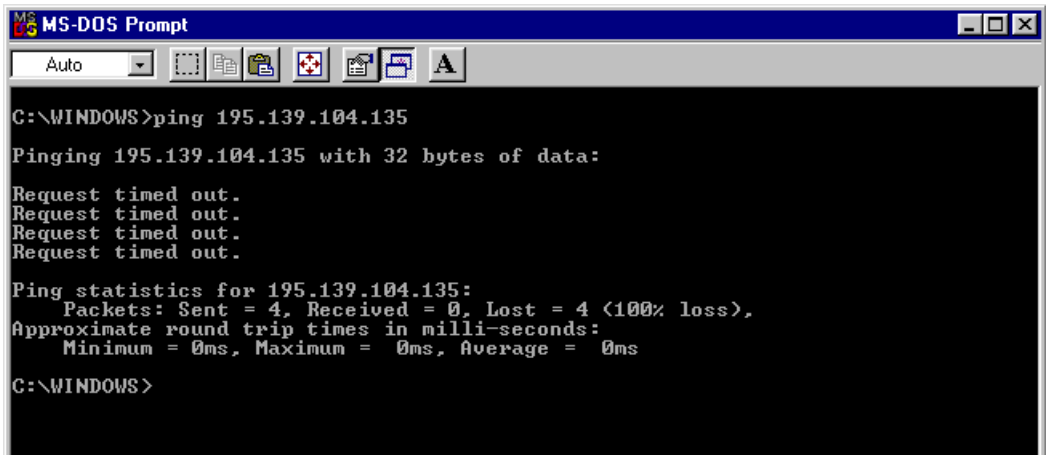

MS-DOS Prompt
Auto
C:\WINDOWS>ping 195.139.104.135
Pinging 195.139.104.135 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 195.139.104.135:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\WINDOWS>

Figure 4-13 Ping time-out.

Shell

Accessing the shell can sometimes be useful if you want to use command-line tools. This is only recommended if you are an experienced UNIX or Linux system administrator. It can be of great help if you gain familiarity with some of the most used tools (see "Using ssh in MS Windows" on page 115 for more information on using third party tools).

To access the shell, you must select the **Shell**-button in the firewall console. This will send you to the shell, and once you are there, you have to type `exit` to go back to the firewall console. Note that this will not exit the firewall, only go back to the console.

Installing the Firewall Client

The Firewall client software can be installed on any of the following operating systems:

- Linux
- Windows 95
- Windows 98
- Windows NT 4.0
- Windows 2000
- Windows XP

We recommend that you close all running programs prior to installing.

Installing the Windows Firewall Client

1. Insert the Trustix Firewall CD-ROM into the CD-ROM drive of the computer that is going to be used to administer the firewall.
2. Normally the installation will start automatically. If not, start the program `\FirewallSetup.exe` on the CD-ROM.
3. Follow the on-screen instructions to select and install the desired components.

Installing the Linux Firewall Client

Installing the Linux client software consists of these steps:

1. Mount the Firewall CD-ROM. In the following instructions, we will assume it is mounted on `/mnt/cdrom`.
2. Install the log viewer client.
3. Install a suitable Java VM, if you haven't done so already.
4. Install the firewall client. This can be done as a system-wide installation or as a user-local installation.
5. Unmount the CD-ROM:
   ```
   # umount /mnt/cdrom
   ```

The details of these steps are as follows:

Installing the Log Viewer Client

The log client software consists of 3 RPM packages. As root, install all of them, using the following command:

```
# rpm -Uvh /mnt/cdrom/xploy-*.rpm
```

The log client can now be started with the command:

```
# /opt/xploy/bin/xploy
```

Installing the Java Virtual Machine

We recommend using the IBM Java VM supplied on the CD-ROM. As root, install it using the command:

```
# rpm -Uvh /mnt/cdrom/jre/ibm/linux/IBMJava2-JRE-1.3-
1.1.i386.rpm
```

Installing a System-wide Firewall Client

As root, invoke the installation script, using the following command:

```
# /mnt/cdrom/FirewallClientInstaller
```

The script will prompt you for information. Default settings are shown in square brackets [ ]. The script will first prompt you for which Java VM to use:

```
You have the following Java VMs installed:
/opt/IBMJava2-13/jre/bin/exe/java
/opt/IBMJava2-13/jre/bin/java

Which one do you want to use [/opt/IBMJava2-
13/jre/bin/java]:
```

Next, choose the installation directory for the client:

```
Directory for client installation [/opt/xsentry]:
```

We generally recommend `/opt/xsentry` but you can install it elsewhere, like `/usr/local/xsentry`. Finally, a symbolic link to the client program will be created:

```
Command pathname for running firewall client
[/opt/bin/firewall]:
```

As the log viewer is already located in `/opt/bin`, we suggest you accept the default and add `/opt/bin` to your $PATH. The firewall client can now be started by typing:

```
$ /opt/bin/firewall
```

Installing a User-local Firewall Client

This installation is only suitable if a single user is to use the client. The installation steps are very similar to the system-wide installation, except that the software is now installed in a user directory, and is owned by the user that installed it.

Log in as that user (assuming "jsmith" below), and type:

```
$ /mnt/cdrom/FirewallClientInstaller
```

The Java selection step is the same as for system-wide installation. As installation directory, it will suggest a separate directory under $HOME:

```
Directory for client installation [/home/jsmith/xsentry]:
```

The command symlink is then suggested located in `~/bin`:

```
Command pathname for running firewall client
[/home/jsmith/bin/firewall]:
```

The firewall client can now be started by the command:

```
$ ~/bin/firewall
```

De-installing the Windows Firewall Client

Choose **Start > Settings > Control Panel > Add/remove program**. Mark Trustix Firewall 3 in the list of programs and click **Change/Remove** in Windows 2000, **Add/Remove** in earlier Windows versions:

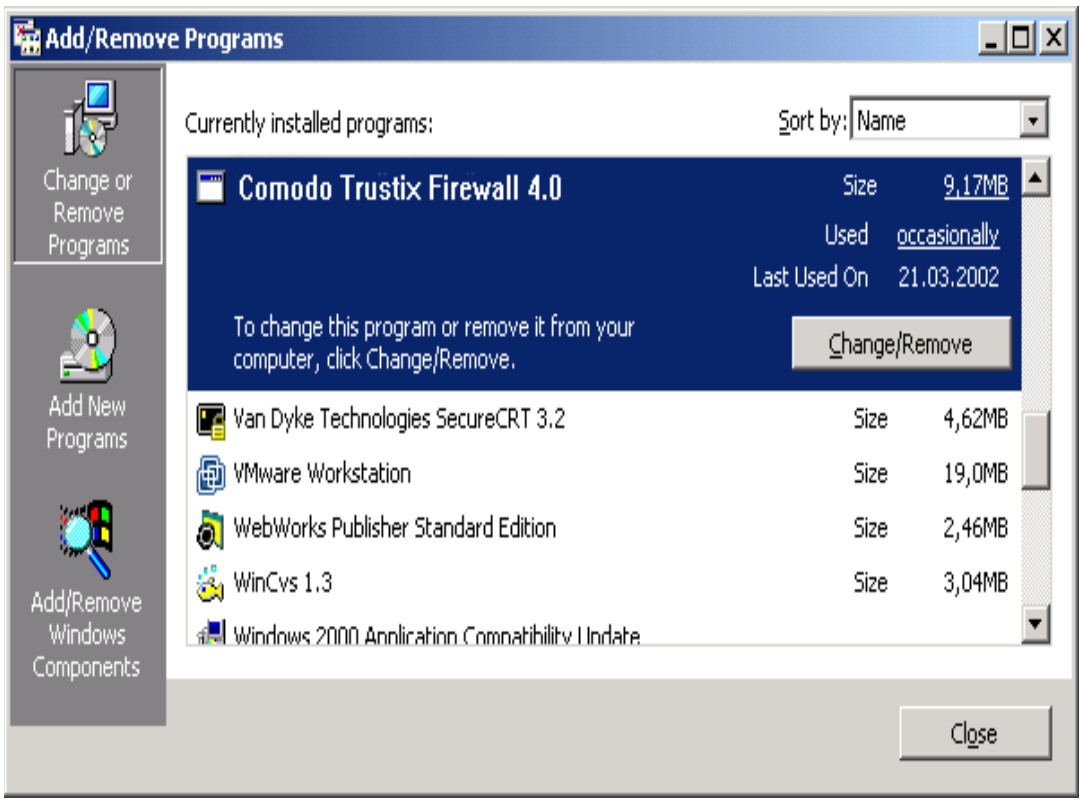


Figure 4-14 Uninstall Windows Firewall Client

De-installing the Linux Firewall Clients

The RPM packages are uninstalled using the `rpm -e` command.

Log client: `# rpm -e xploy-client xploy-log-client xploy-libs`

Java VM: `# rpm -e IBMJava2-JRE`

The firewall client is uninstalled by removing the installation directory, command symlink, and configuration file. The following assumes you accepted the default installation directory:

System-wide uninstall:

```
# rm -rf /opt/xsentry /opt/bin/firewall /etc/xsentry.conf
```

User-local uninstall:

```
$ rm -rf ~/xsentry ~/bin/firewall ~/.xsentry.conf
```

Installing the Firewall License

General Licence Issues

The following is a guide through the process of generating and installing the licenses for the Trustix Firewall. The licenses are generated and downloaded from:

`http://trustix.com/purchase/index.html`

Before starting to install the licenses you have to:

- Install the Trustix Firewall Server on your firewall.
- Do the basic firewall server configuration. See “Configuring the Firewall Console” on page 44.
- Install the Trustix Firewall Client on an administration host.

Getting the Licence Key

To generate a license for your Trustix Firewall, you will have to go though the following steps.

1. Enable License Negotiation

You will have to set up the firewall server to listen for and accept license negotiation requests from the firewall client. In the firewall console, scroll through the main menu, and select **Enable license negotiation**. Then select **OK**.

2. Log on to the Server from the Administration Client

Before you can log on to the server from the administration client, a remote administrator must have been defined. This was done a part of the basic firewall configuration. See “Define Remote User” on page 46. When you start the firewall administration client, you will be prompted for name and password for the remote administrator. See Figure 4-15 on page 55.

Figure 4-15 Log on to the firewall

3. Find Your System Key

When you log on to the firewall administration client the first time, the client will detect that you haven't yet licensed the firewall. Clicking OK will take you through to panel where the System Key (or MAC Address) is presented, copy the number for use when applying for your license at the following URL.

`http://trustix.com/purchase/index.html`

For further details on how to install your license, please refer to the licensing section of the quickstart guide on page XVIII

Trustix™

Chapter 5

Using the Firewall Console

This chapter explains how to use the firewall console. This console is either presented to you through a terminal application or through the monitor connected to your firewall server.

If you want to administer the firewall through a terminal application you first need to log on to the server, providing the password set during installation. To start the Firewall Console type:

```
$ xsadm
```

System Password

To prevent unwanted users from tampering with the firewall's settings, the user has to be authenticated before being allowed access:

Figure 5-1 Console login screen.

Menu Administration

After authenticating, the scrollable administration menu (Figure 5-2 and Figure 5-3) is shown. This chapter presents the operations that are possible from the firewall console.

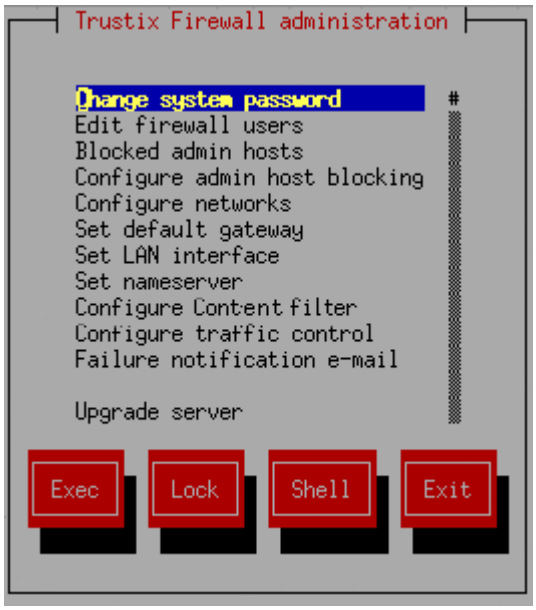


Figure 5-2 Console menu.

Figure 5-3 Console menu, scrolled.

Note that only the features of the firewall that you have a license for will be available in the menu. You move up and down the main menu by using the arrow keys. <Tab> moves the cursor to the buttons seen at the bottom of the menu, while <Space> and <Enter> selects.

The buttons have the following functions:

- **Exec** - executes the line that is highlighted in the firewall console.
- **Lock** - finishes this session with the firewall console. Always use this option after configuring the firewall. If not used, unauthorized users can alter the settings of the firewall. Selecting Lock makes the authentication dialog (Figure 5-1, "Console login screen.," on page 57) reappear.
- **Shell** - opens a full-screen shell. Note that you should not leave the administrator host in shell mode as the host is not locked. To return to the main menu, type

  ```
  exit
  ```

- **Exit** - closes the firewall console if remote access is used.

Change System Password

Used for changing the root (administrator) password, of the firewall. This password is used to authenticate the administrator at the console, and when logging in using ssh.

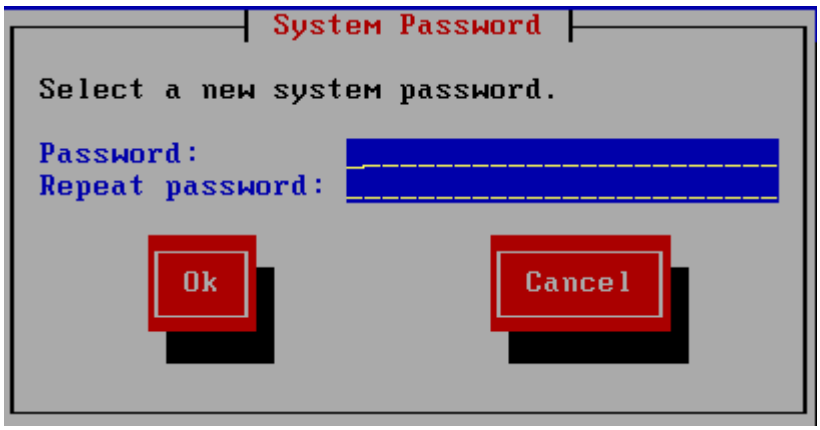


Figure 5-4 Change system password.

Edit Firewall Users

Allows the administrator to add, modify or delete remote administrators of the firewall. Remote administrators can be granted access to configure the firewall using the firewall administration client, and to inspect and analyze logs using the log module. You must specify login name and password for each user, as well as the IP addresses of users' workstations (Figure 5-5, Figure 5-6 and Figure 5-7).

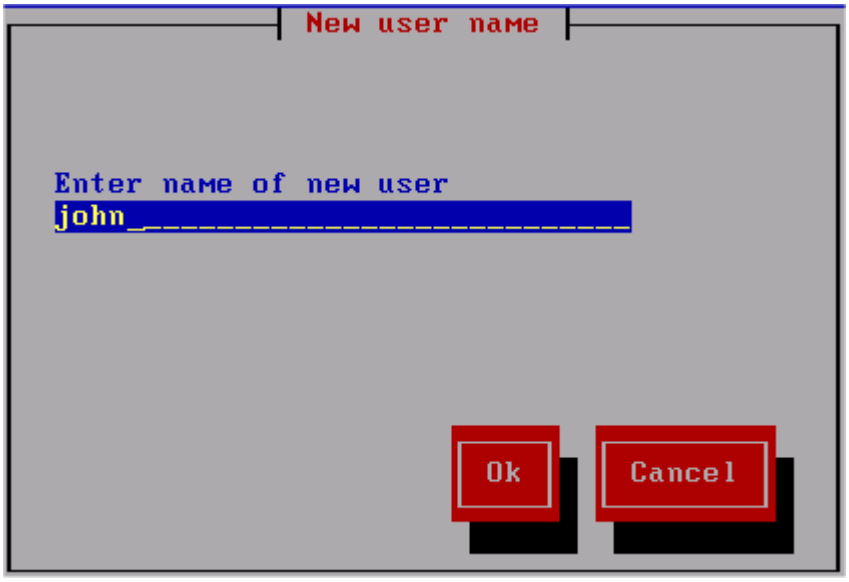


Figure 5-5 Add firewall user.

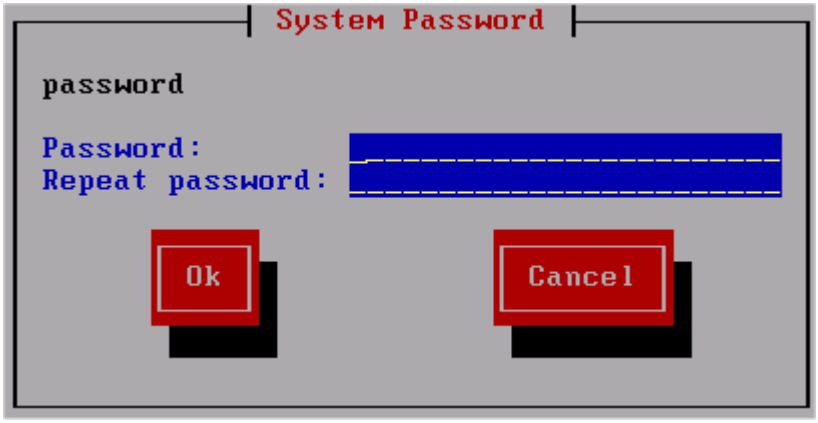


Figure 5-6 Enter password for firewall user.

Figure 5-7 The IP which the Firewall user can administrate the firewall from.

The IP addresses must be separated by commas. Do not use blanks.

Re-enable Blocked Administration Hosts

An administration host is automatically blocked after a specified number of failed authentication attempts within a specified time limit. This selection lets the administrator re-enable any blocked hosts. This can only be done with xsadm at the console.

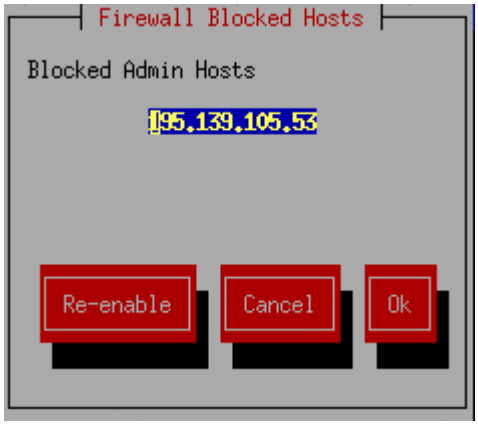


Figure 5-8 Blocked admin hosts.

Configure Administration Host Blocking

An administration host is automatically blocked after a number of failed authentication attempts within a time limit. This selection lets the administrator specify a limit on the number of failed logins, as well as a time period for the limitation:

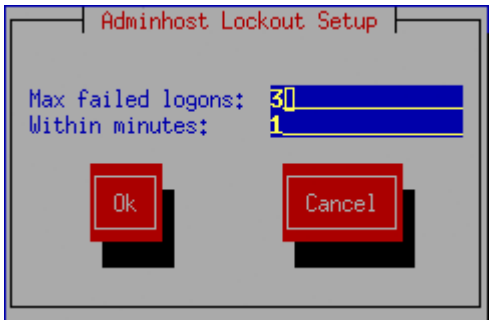


Figure 5-9 Configure admin host blocking.

Configure Networks

This selection lets the administrator configure the network support of the firewall. The necessary settings were set during installation, see “Firewall Server Installation” on page 31. Use this menu if you need to change settings such as IP addresses, netmasks etc. It is also where you name the zone.

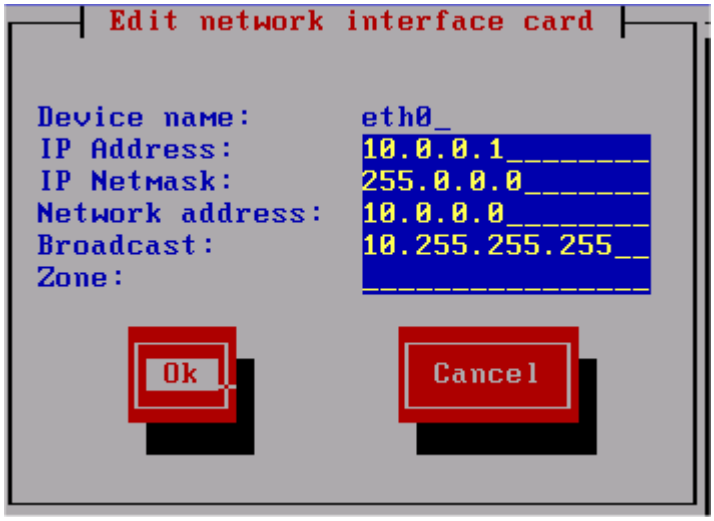


Figure 5-10 Configure networks.

Set Default Gateway

Here you define the IP address used as the firewall’s default gateway, and which interface it is connected to.

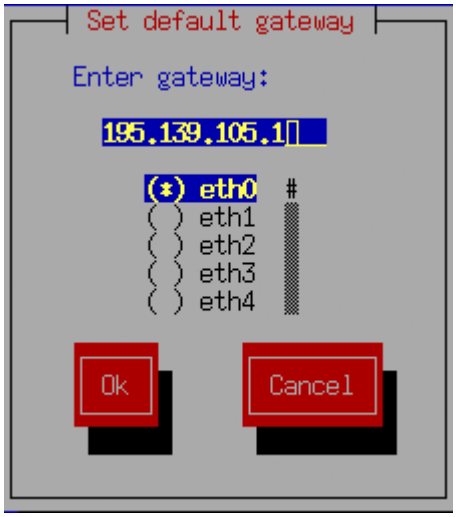


Figure 5-11 Set default gateway.

Set LAN Interface

A list of network interface cards will be shown. Choose the network interface card that should belong to the LAN. One interface will not appear in the list, this is the interface that has been marked as the default gateway interface.

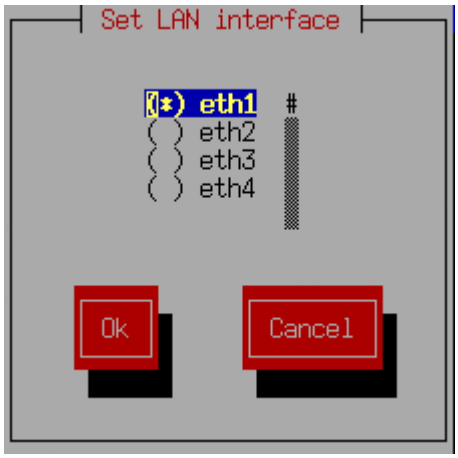


Figure 5-12 Set LAN interface.

Set Name Server

This selection lets the administrator define the primary and secondary domain name servers for the firewall.

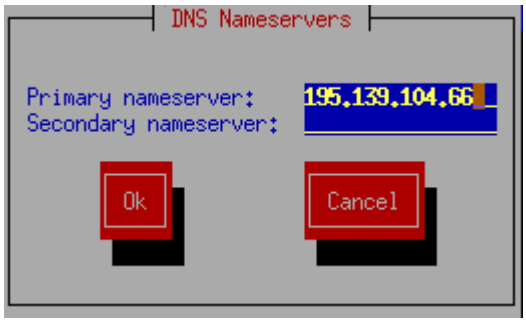


Figure 5-13 Set name server.

Configure Filtering Proxy

The Trustix Firewall has a built-in filtering proxy. It works both as an content cache to speed up your Internet access, and as a URL and content filter. This selection lets the administration enable the proxy, and select whether the proxy should be used for the LAN zone only, or for all zones.

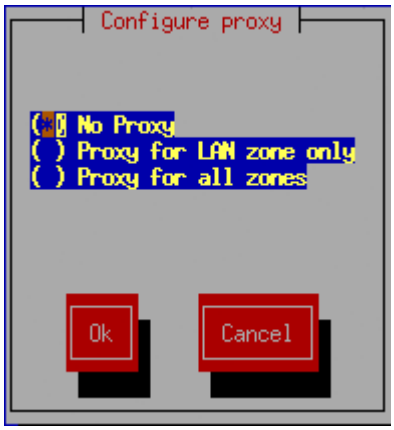


Figure 5-14 Configure filtering proxy.

Configure Traffic Control

The Trustix Firewall has a framework for traffic control that can be easily extended to suit your particular needs. The Configure Traffic Control menu allows you to select one of a set of predefined traffic shaping scripts.

All executable scripts located in the directory `/opt/xsentry/etc/tcscripts` will appear in the traffic control menu.

The predefined selection "--None--" will disable traffic shaping on all net-work interfaces. If another script is selected, that script will be run immediately, and in addition be scheduled for running during start-up whenever the system is rebooted.

You write the scripts yourself, according to your particular quality of service requirements. Use the `tc` command for doing the traffic shaping. More information can be found on the Linux Advanced Routing & Traffic Control project homesite at:

`http://lartc.org`

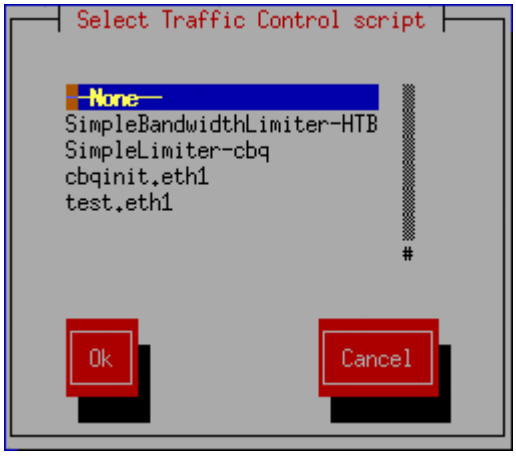


Figure 5-15 Configure traffic control.

Failure Notification

The Trustix Firewall is capable of monitoring its own critical processes, as well as monitoring its peer firewall, in a fault-tolerant setup. When a critical problem is detected, the firewall will try to restart dead processes. In a fault-tolerant setup, if the master is dead, the slave will take over. In both cases the firewall can be configured to send an e-mail warning.

This selection lets the administrator set up e-mail address(es) to be notified when failures occur. Each field can contain a single e-mail address or a comma-separated list of addresses (no spaces).

Figure 5-16 Failure notification e-mail.

Upgrade Server

The Trustix Firewall can be automatically upgraded. Selecting Upgrade Server will present you with a confirmation dialog:

Figure 5-17 Upgrade server.

If you accept, all relevant updates will be downloaded from `www.trustix.com` and installed. An information screen with a listing of all upgraded modules will be shown. When you click **OK**, you will be informed that xsadm has to restart to complete the upgrade. Click **OK** to restart.

Shutdown Firewall

Selecting this option will causes the firewall to shut down. All traffic between the networks will be stopped. The user will be prompted with a dialog box asking if the firewall should be shut down.

Figure 5-18 Shutdown firewall.

Block/Unblock Traffic

The firewall blocks all traffic through the firewall. The administrator is asked to confirm this action. When the firewall is blocking all traffic, this menu item is replaced by the new item **Unblock traffic**. When selecting this, the firewall reactivates the administrator's configuration.

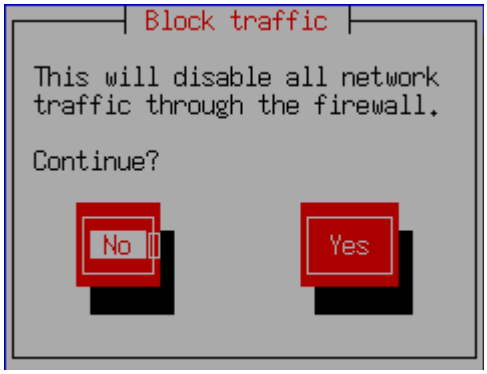


Figure 5-19 Blocking network traffic.

Enable/Disable Ping Testing

The firewall replies to ping requests while the ping test mode is enabled. If you choose to enable ping testing, the main menu item changes to **Disable ping testing** until you change it back.

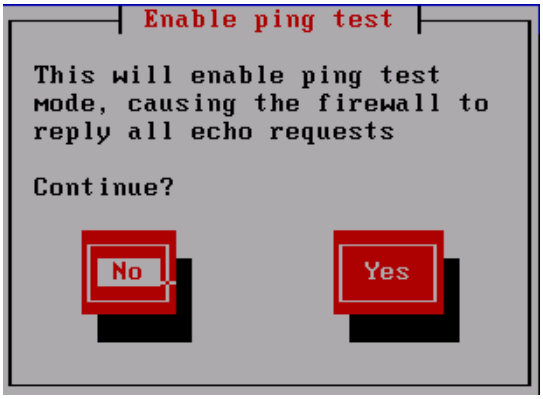


Figure 5-20 Entering ping test mode.

Enable/Disable Remote SSH

Makes the Firewall users able to connect to and administer the firewall through an SSH connection. If remote SSH is enabled the menu text is changed to **Disable remote SSH**.

The ssh daemon runs on port 350 (Normally it runs on port 22).

The Firewall users must log on to the Firewall server as root. There is no security risk since only predefined IP addresses are allowed to log on. The operating system on the server is a Linux system. Those users already familiar with Linux will be able to use the system to its maximum.

Windows:

The SSH client, which the administrator uses to log on to the firewall, must be configured to use port 350.

Linux:

Log on to the Firewall server with the command:

```
$ ssh -p 350 -l root firewall.trustix.com
```

In Linux, `-p` gives the port number which the ssh daemon runs on and `-l` gives the user name.

If the administrator wants to use port forwarding to another service which runs on port 350, the port number for the ssh daemon has to be changed. The port number is given in the file `/etc/ssh/sshd_config` on the server. When the number is changed run the command:

```
# service sshd restart
```

The ssh daemon will restart on the new port number.

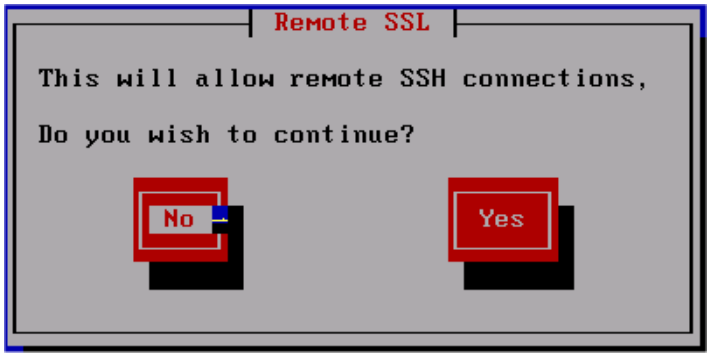


Figure 5-21 Enable remote SSH.

Set Keyboard Layout

In this menu you can set the keyboard layout.

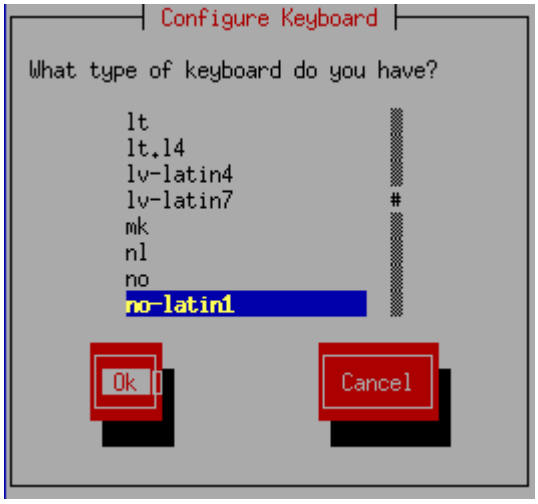


Figure 5-22 Set keyboard layout.

Set Time Zone

Here you can set the time zone.

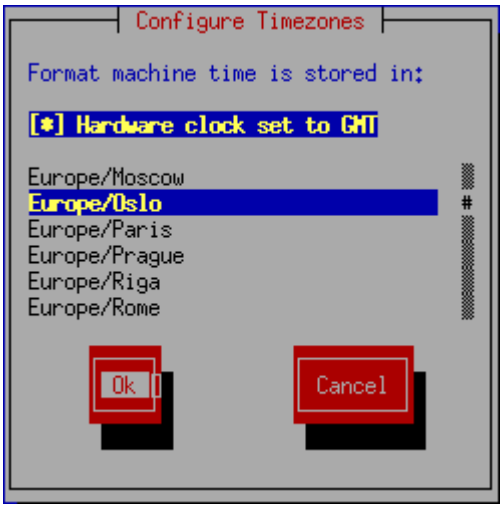


Figure 5-23 Set time zone

Trustix™

Chapter 6

The Firewall Client

The Firewall client is the Firewall's configuration tool. It introduces a revolutionary new way of configuring a firewall. This chapter will introduce the client's easy-to-use visual modeling interface.

This chapter includes the following information:

- Starting the Firewall client
- The client window.
- Detailed explanations of the items to be found in the client window

Starting the Firewall Client

To start the client:

Choose **Start > Programs > Comodo Trustix > Firewall x > Comodo Trustix Firewall**. (If the program was installed in a different folder than **Trustix**, choose that folder from the **Start > Programs** menu. Also, x indicates the firewall version)

The Client Window

The main window (Predefined Services) consists of:

- The menu bar
- The toolbar
- The work area
- The Network view
- The Worksheet
- The status bar

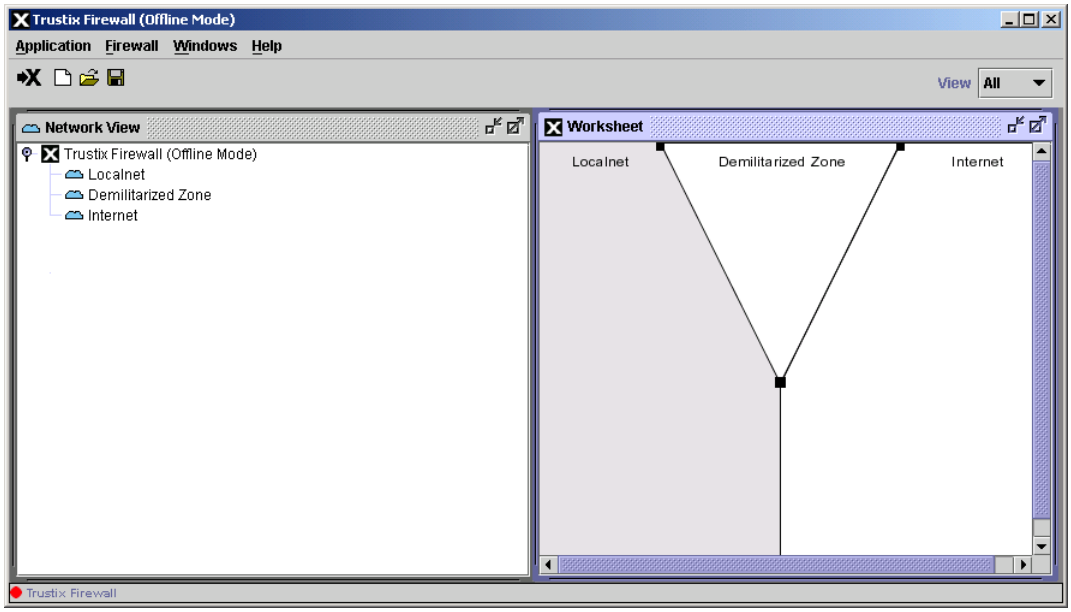


Figure 6-1 Firewall client window.

The Menu Bar

The Menu bar has three drop down menus; **Application, Firewall** and **Help**.

Application

From the **Application** menu, you can install licenses, load and save configurations, backup and restore the system configuration, and more. See Figure 6-2 on page 73.

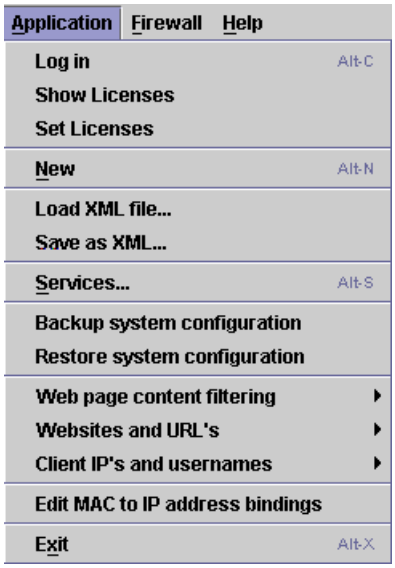


Figure 6-2 Application menu.

Login

In the dialog, you specify the IP address of the firewall, username and password.

Show Licences

Shows information on your license status, e.g. how many zones you are allowed to use.

Set Licenses

Opens the dialog for updating your license and allows you to select and load the updated license file.

New

Clears the current configuration of your firewall to define a new configuration.

Load XML File...

It is possible to have several configurations. When reopening your client, use this option to load previous setup.

Save as XML...

Saves the current configuration to file. Use this feature to backup your configuration.

Services...

From here, new services can be defined and edited. This is described on page 117 and onwards.

Backup System Configuration

Backs up the firewall system configuration locally on the client host.

Restore System Configuration

Restores a previously saved system configuration from the client host back to the firewall.

Websites and URLs

Here you can edit black lists and white lists for the URL filter in the firewall. The sub-selections are:

- Block these URLs
- Always permit these URLs
- Block these sites
- Always permit these sites

Client IPs and User Names

Here you can edit black lists and white lists for the IP address and user filter in the firewall. The sub-selections are:

- Block these IP addresses
- Always permit these IP addresses
- Block these users
- Always permit these users

Edit MAC to IP Address Bindings

Here you can set up static bindings between MAC addresses and IP addresses. The format is the same as for the `/etc/ethers` file: MAC address first, then IP address.

Exit

Exits program. Before exiting, the program prompts if the current configuration should be saved.

Firewall

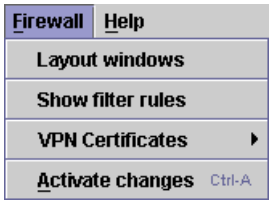


Figure 6-3 Firewall menu.

Layout Windows

Maximizes the Network view and Worksheet within the work area.

Show Filter Rules

Shows details of current rules on firewall.

Example:

```
1 DENY tcp   ------  20.0.0.0/16   10.0.0.0/16    * -> *
```

The columns show from left to right: Number, action, protocol, flags, source address, destination address and source port -> destination port.

VPN Certificates

Have three sub-choices: CA Certificates, User Certificates and Revoked Certificates. See page "Predefined Services" on page 117 for details on how to create and administer CA certificates.

Activate Changes

Sends the rules, which are set in the client to the firewall, and activates them. The rules specified in the worksheet won't be activated until this option is selected.

Help

About

Displays information about this version of the Firewall client.

The Toolbar

The toolbar offers quick access to commonly used operations.

Figure 6-4 The toolbar

Table 6-1 Toolbar buttons.

Button	Operation
	Activate rules on the firewall. The current configuration is saved, sent to the firewall and activated
	Clear configuration. A clean worksheet will appear, but the existing rules will not disappear before activating the new empty worksheet.
	Open file. Loads a previously saved configuration from disk.
	Save file. Saves the current configuration to disk.
	Select type of rules to show in the worksheet. This is useful when checking rules for correctness in a crowded worksheet.

The Work Area

The work area contains two windows. Both windows can be moved and resized to suit personal preference. The layout will be saved when the program is closed.

Worksheet

The worksheet is the window that contains the visual representation of the security policy on the firewall.

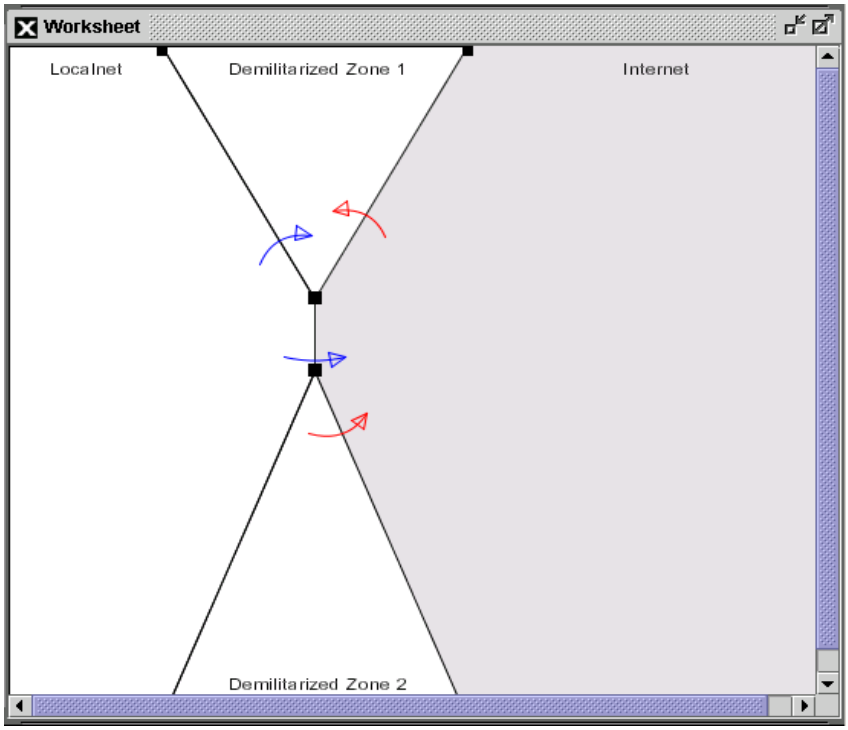


Figure 6-5 The worksheet.

This is where most work configuring the firewall is done. The worksheet is divided to represent the zones. Up to four zones can be shown at the same time. A zone is selected by clicking in the zone, and the active zone changes color to gray.

Icons in the worksheet represent the nodes. A node is moved by dragging it around. All nodes have an icon. The service nodes have independent icons. These are also used as icons for the server class. The services shown here are the most commonly used, a complete list is provided on page 117, including an overview of protocol and default port usage.

Table 6-2 Worksheet icons.

Icon	Description
	Host / VPN Gateway
	Server
	Host folder

Table 6-2 Worksheet icons.

	Subnet
	AUTH
	DNS - The Internet Domain Name Service
	Generic UDP - User Datagram Protocol
	FTP – File Transfer Protocol
	HTTP - The World Wide Web
	HTTPS – Secure WWW
	IMAP4 – Internet Message Access Protocol
	NNTP – News service
	POP3 - Post Office Protocol 3
	SIMAP – Secure IMAP
	SMTP - Simple Mail Transfer Protocol
	SSH - Secure shell
	Windows Directory Service
	Windows Networking

The rules are shown in the worksheet as arrows pointing in the direction of the network traffic. A blue arrow indicates *allowing* traffic in that direction. A red arrow indicates *denial* of traffic in the pointing direction. A dotted blue arrow indicates that the traffic in that direction is *allowed and masqueraded.* A green arrow indicates a *VPN connection* that is *activated* and a dotted green arrow indicates a *VPN connection* that is *disabled*.

It is possible to add breakpoints to rules for increased flexibility. Add a breakpoint to a rule by locating the spot on the arrow where the breakpoint should be added. Then simply click and pull the arrow into the desired shape. To remove a breakpoint, simply make the arrow straight by moving the node, or click the right mouse button on the arrow, and select Stretch.

The Network View

The network view contains a tree structure, which reflects the structure of the firewall configuration.

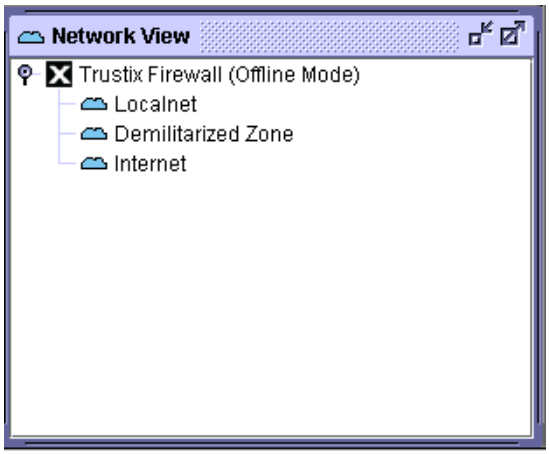


Figure 6-6 The network view.

The first time the client is started, it contains only the names of the zones. When nodes are added to the worksheet, they will appear organized in the tree hierarchy. The Network view shows all zones used, up to the maximum of 128. By right clicking on a zone not currently viewed in the Worksheet, the following drop down menu appears:

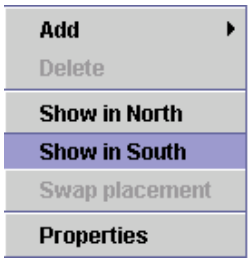


Figure 6-7 Show zones.

Show in North/South means that the rules for this zone are shown in, respectively, the upper or lower part of the worksheet.

The rules are put under the source nodes of the rule. In addition to the icons used in the worksheet, the following are used in the Network view:

Table 6-3 Network view icons.

Icon	Description
	Firewall
	A zone
	Deny rule
	Allow rule
	Masquerade rule
	Portforwarding
GW:	VPN Gateway

Trustix™

Chapter 7

The Firewall Administration Application

This chapter contains information on how to configure the firewall after installation, and how to do standard configuration operations. It will show that most operations are available directly from the worksheet.

This chapter covers the following sections:

- Start-up
- Configuration basics
- Operations
- Example rules
- Advanced options

Start-up

The client needs to be connected to the firewall before any configuration can be done. At startup the Firewall client will show the login dialog.

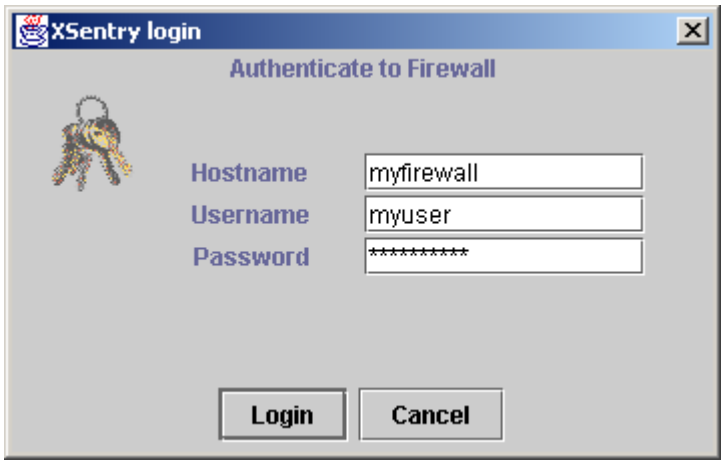


Figure 7-1 Login dialog.

Fill in the IP address or the DNS name of the firewall, Username and the Password that was set when the firewall was installed, and click **Login**.

Configuration Basics

After installation, the firewall needs to be configured to reflect the organization's security policy. Configuring the firewall consists of 3 simple steps:

1. Adding all nodes to the worksheet.
2. Setting all rules.
3. Activate the rules on the firewall.

Note that the nodes and rules that you add to the worksheet are not activated automatically. When you have finished adding nodes and rules, the new configuration must be sent to the firewall. do this by selecting **Firewall > Activate Changes**, or click the **Activate** button on the Taskbar.

Operations

Adding a Node

Nodes are added directly from the worksheet or the network view. Click the right mouse button on the zone's icon in the network view or simply click the zone in the worksheet itself, and select **Add > Host, Hostfolder, Server, Serverclass, Service, Service Folder, Subnet, Road Warrior** or **VPN Gateway**.

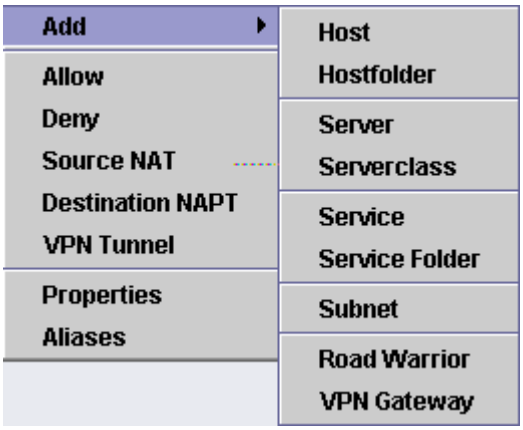


Figure 7-2 Add node pop-up menu.

Adding a Host

The **Add Host** dialog appears. Enter the name of the host. This is the name that will be shown in the administration client, not to be confused with a DNS name. Then enter the IP address or the hostname of the host.

You may also enter the MAC address of the host. Then the firewall will reject all traffic for this host where the IP address and the MAC address do not match as specified. Click **OK** to add the host to the worksheet.

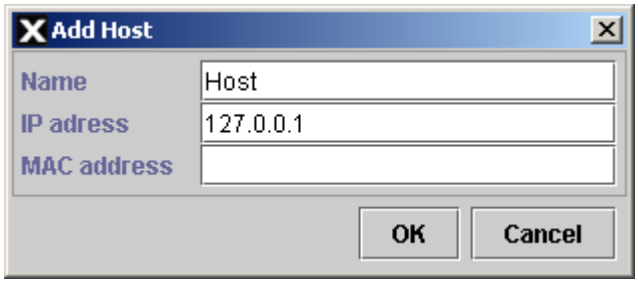


Figure 7-3 Properties for host.

Note: If a dynamic IP address allocation server is used, setting rules for hosts will have no meaning. Please study "Concepts" on page 1 for more information regarding this problem.

Adding a Service

A list of services will appear. Select the type of service from the list, and click **OK**.

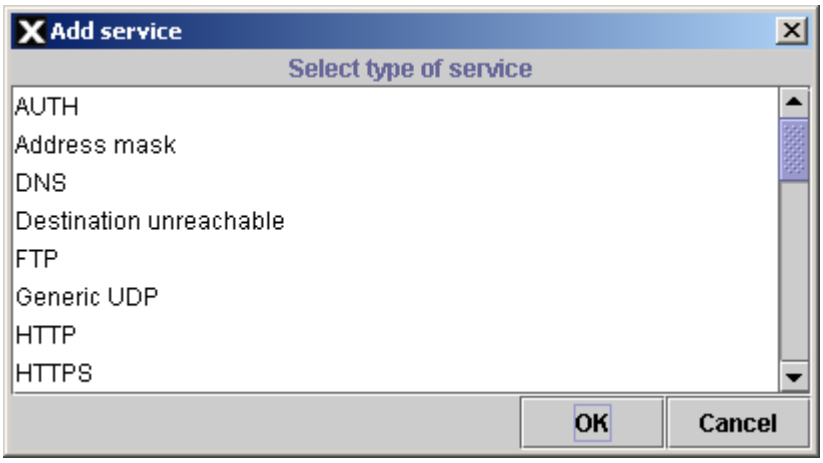


Figure 7-4 Add service.

Adding a Server

The **Add Server** dialog appears. Enter the name of the server. This is the name that will be shown in the administration client, not to be confused with a DNS name. Then enter the IP address or the hostname of the server.

You may also enter a Network Address Translation (NAT) alias for the server. If an alias is given, then any allow rules involving this server will be translated to destination NAT rules from the IP alias to the real IP address for this server.

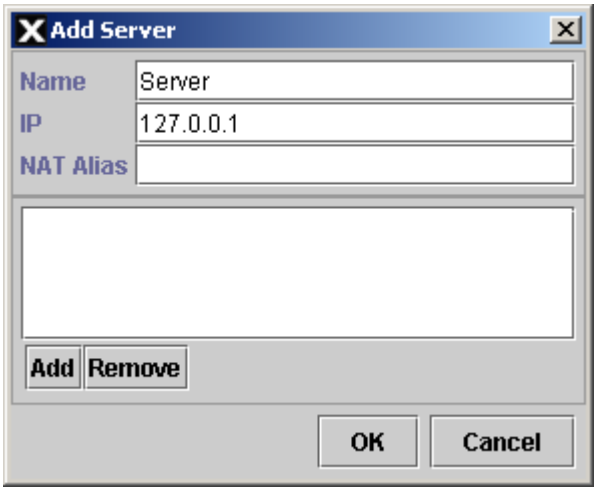


Figure 7-5 Properties for server.

To edit the list of services for this server, click **Add** to add new services. To remove a service highlight it select **Remove**. Select **OK** to add the server to the worksheet.

Adding a Subnet

The **Add Subnet** dialog appears. Enter the name, network address, network mask and broadcast address for the subnet.

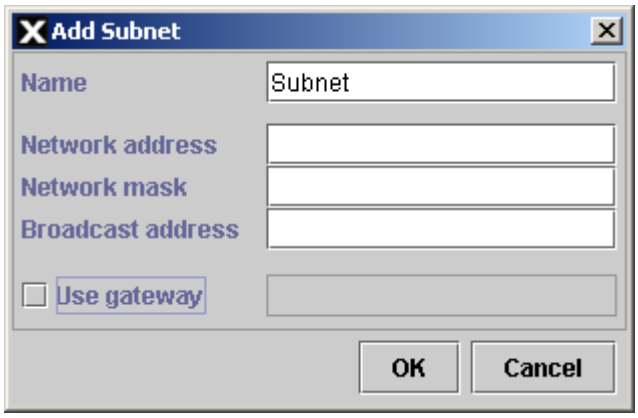


Figure 7-6 Properties for subnet.

Tick the **Use gateway** field and specify the gateway to be used, if relevant. Click **OK** to add the subnet to the worksheet.

Adding a Server Class

The **Add Serverclass** dialog appears. Enter a name for the server class. Select the type of service for this server class from the pop-up menu. Selecting several services is not possible.

You may also enter a Network Address Translation (NAT) alias for the server class. If an alias is given, then any allow rules involving a server in this service class will be translated to destination NAT rules from the IP alias to the real IP address for this server.

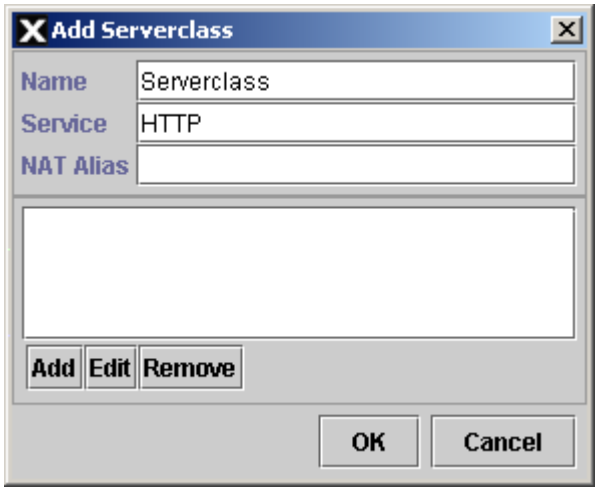


Figure 7-7 Properties for server class.

To edit the list of servers for this server class, click **Add** to add new servers. Hostname and IP address must be given. Click **Remove** to remove servers and **Edit** to change hostname or IP address. Click **OK** to add the server class to the worksheet.

Adding Host Folder

The **Add Host folder** dialog appears. Enter the name for the host folder.

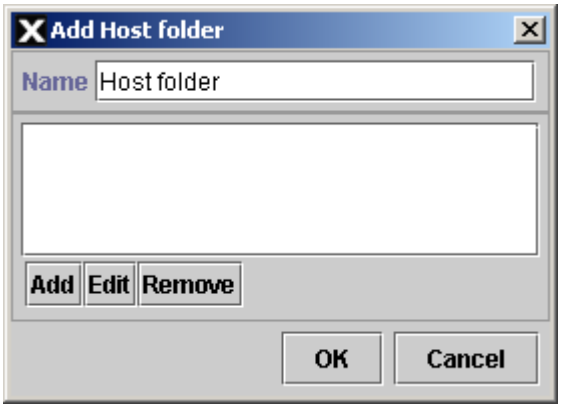


Figure 7-8 Properties for host folder.

To edit the list of hosts for this host folder, click **Add** to add new hosts. Hostname and IP address must be given. Click **Remove** to remove hosts and **Edit** to change hostname or IP address. Click **OK** to add the host folder to the worksheet

Adding VPN

The Firewall can act as a VPN gateway - a VPN tunnel endpoint - for several concurrent VPN connections.

To create a VPN connection between two Firewalls, the following must be done on both Appliances (using the Firewall Client):

- Create a VPN Gateway entity in the actual zone (normally the Internet zone), or right-click an existing VPN Gateway entity to view its properties. If you create a new entity, first type a name in the Name field in the upper left corner of the dialog. See Figure 7-9 on page 88.
- Click **Add** to define a new VPN connection. This opens the dialog shown in Figure 7-10 on page 89. In this dialog, fill in:
  - Identity: This is used by the VPN subsystem on the appliance server to uniquely identify this connection.
  - IP Address: The IP address of the other VPN Gateway that we want this gateway to connect the tunnel to.
  - Their Subnet: This is the IP address range the VPN Gateway on the other end of the VPN connection will give us access to.
  - Our Subnet: This is the IP address range we want this VPN Gateway to give the other end access to. This parameter is optional, and if it is left out, the system will select the address range of the zone in which the VPN tunnel arrow ends.
  - Auth Method: Either

    Shared Secret: A password consisting of no less than 8 characters. The password must be the same on both VPN Gateways

    or

    X.509: Select a certificate from the server's certificate store that the other VPN Gateway will identify itself with. See “Creating Certificates” on page 131 if you choose this alternative.

    Click OK to submit the data to the VPN Gateway entity.

Note: *After successfully negotiating a VPN tunnel, any computer behind our gateway that has an IP address within the range given in Our Subnet will be able to freely communicate with any computer that has an IP address within the range given in Their Subnet, if that computer is reachable from the gateway on the other end.*

- When you are satisfied with the setup, click OK to close the VPN Gateway Setup dialog.
- If necessary, create a VPN tunnel rule from the VPN Gateway entity to the desired zone, by right-clicking on the entity or in the zone, and activate the rule by right-clicking on it.
- Finally, transfer the setup to the Firewall Server.

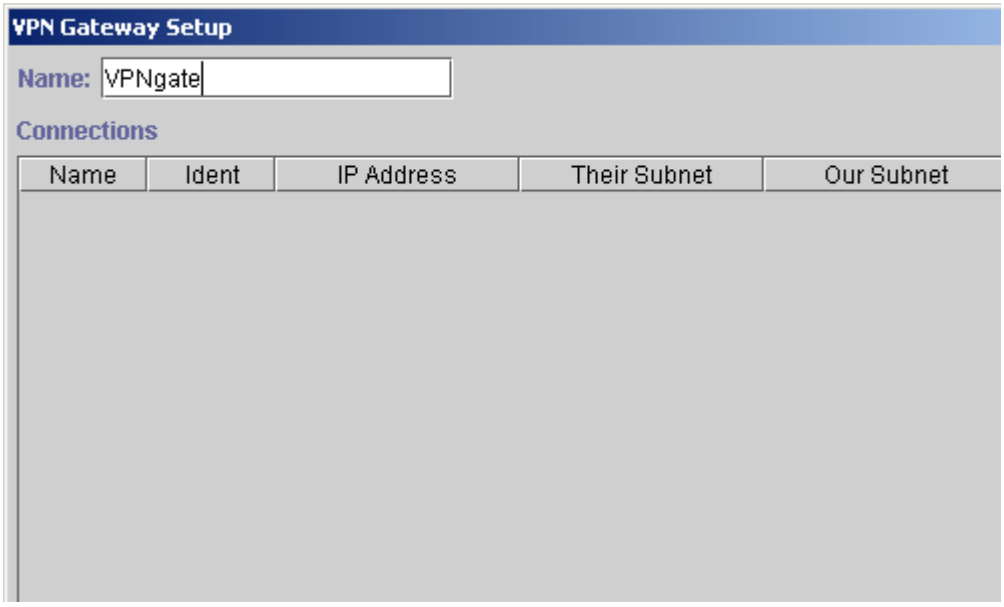


Figure 7-9 Add VPN Gateway.

Remove an already added connection by marking it and click **Remove**. The **Edit** button displays the dialog box in Figure 7-10.

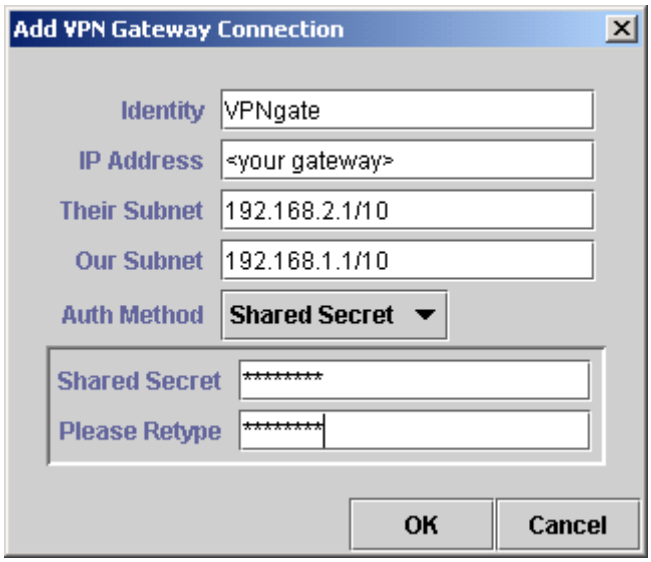


Figure 7-10 VPN Gateway Setup dialog.

Removing a Node

To remove a node click the right mouse button on the node, and select **Delete**. When deleting a node, all rules associated with that node are deleted.

Changing the Properties of a Node

To review or change the properties of a node, click the right mouse button on the node, and select **Properties**. This will make a properties dialog appear. The appearance of this dialog will depend on the type of node selected. Figure 7-11 shows one example of a properties dialog.

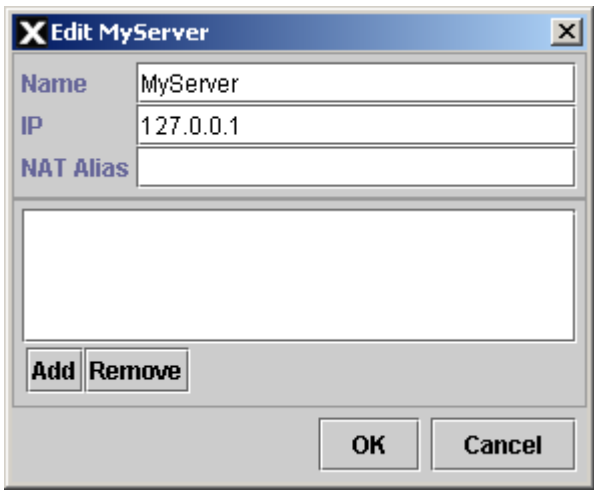


Figure 7-11 Host properties.

For most nodes, all properties can be changed. Figure 7-11 shows Properties for *MyServer*. To remove a service for the server, highlight it and click **Remove**. To add a service, click the **Add** button, and select the service you want to add. To change IP address, click **IP** and enter the new address.

Setting Rules

To add a rule:

1. Click the object the rule should start from (source node or zone) with the right mouse button.

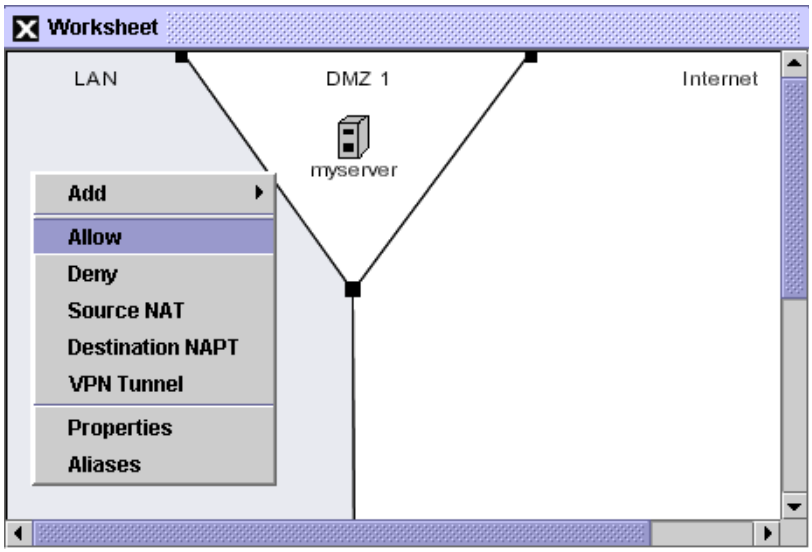


Figure 7-12 Select rule.

2 Select the type of rule that is going to be set (Allow, Deny, Source NAT, Destination NAPT or VPN tunnel). Here Allow is selected.

3 Move the pointer to the destination object, and click the mouse button.

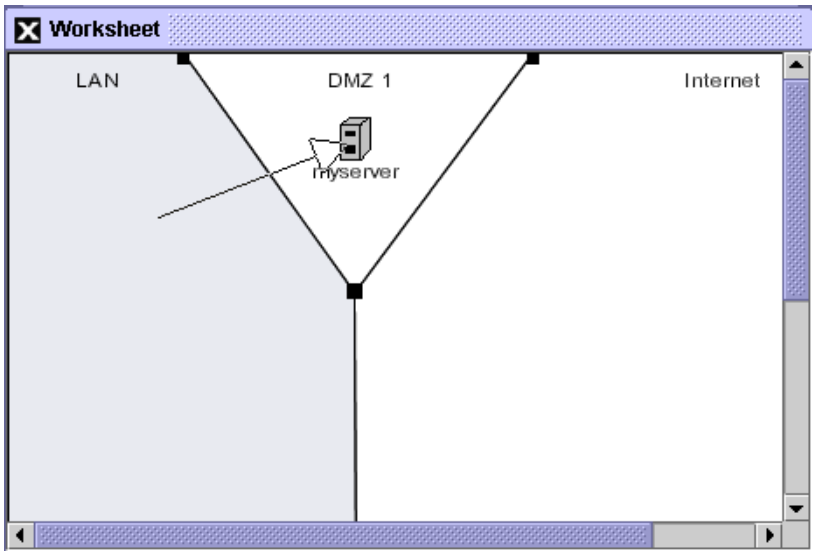


Figure 7-13 Set destination.

4 If the rule is legal, an arrow will appear between the objects, from source to destination.

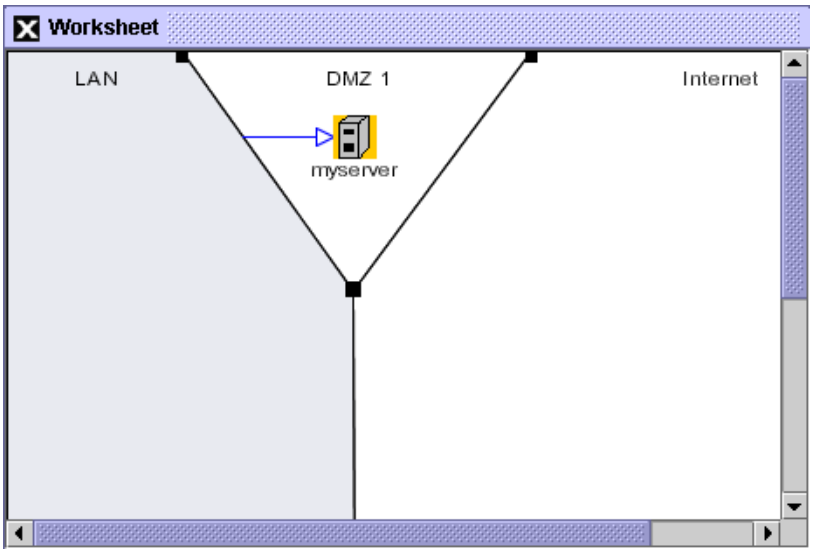


Figure 7-14 Rule added.

Make sure you understand the principles of rules and nodes before setting rules. See “Concepts” on page 1.

Changing the Properties of a Rule

To review or change the properties of a rule, click the right mouse button on the node, and select **Properties**. This will make a properties dialog appear. The appearance of this dialog will depend on the type of rule selected. Figure 7-15 shows one example of a rule dialog.

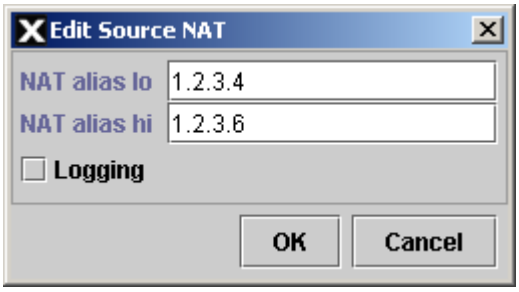


Figure 7-15 Source NAT properties.

For Deny, Allow and Source NAT rules, one can also extend the rule to apply to more protocols than TCP. Just right-click the rule, and tick off **All Protocols**.

Deleting Rules

To delete a rule, click the right mouse button on the rule in the worksheet or in the network view, and select **Delete**.

Activating Rules on Firewall

Select **Firewall > Activate rules.** This causes the rules to be sent to the firewall, and activated.

Save Configuration

When you have finished configuring your firewall, save the setup on e.g. a diskette as backup. Use **Application > Save as XML** to do this.

Enable Logging on Rules

Logging can be applied to rules by clicking the right mouse button on a rule, and ticking **Logging**. Rules that are logged, are displayed in bold.

When logging is applied to a rule, every packet that fits this rule generates a log entry. Setting logging on rules can be very helpful, but remember that logging *allow* rules will generate very large log files. It is recommended to add logging to deny rules only.

Rule Examples

This section contains examples of how different entities can be used to create rules.

The Use of Service

The service nodes are used for allowing/denying one kind of service. A service node can only be used as destination in rules.

Example: Give all computers on the LAN access to all web sites on the Internet

1. Add the service *HTTP* to the Internet zone.
2. Add an *allow* rule from the *LAN* zone to the HTTP node.

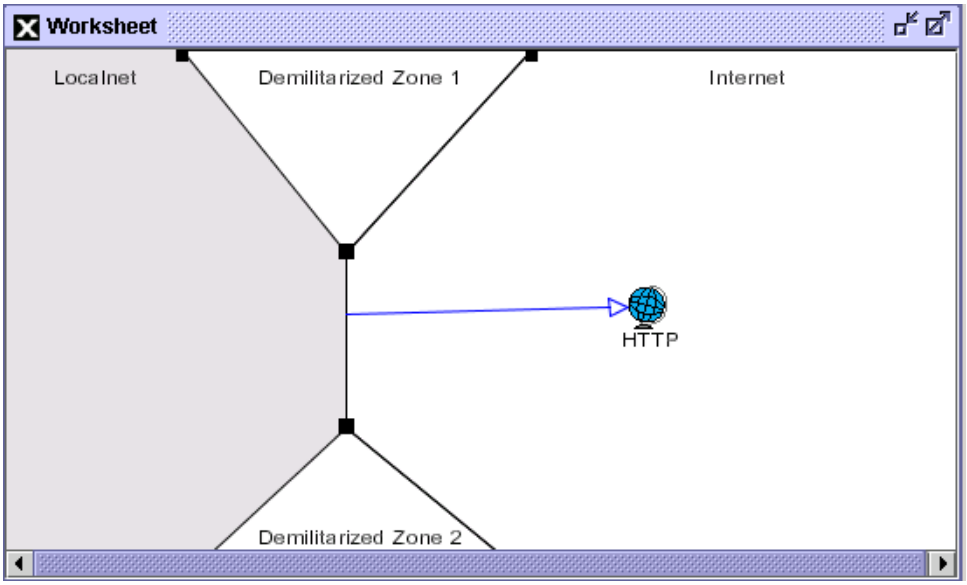


Figure 7-16 All hosts on the LAN can access all web sites on the Internet.

The Use of Hosts

The host nodes are representing computers. They can be used as both source and destination.

Example: Give the host My_host on the LAN access to all web sites on the Internet.

1. Add the service *HTTP* to the Internet zone.
2. Add the host *My_host* to the *LAN* zone.
3. Add an *allow* rule from the host node to the HTTP node.

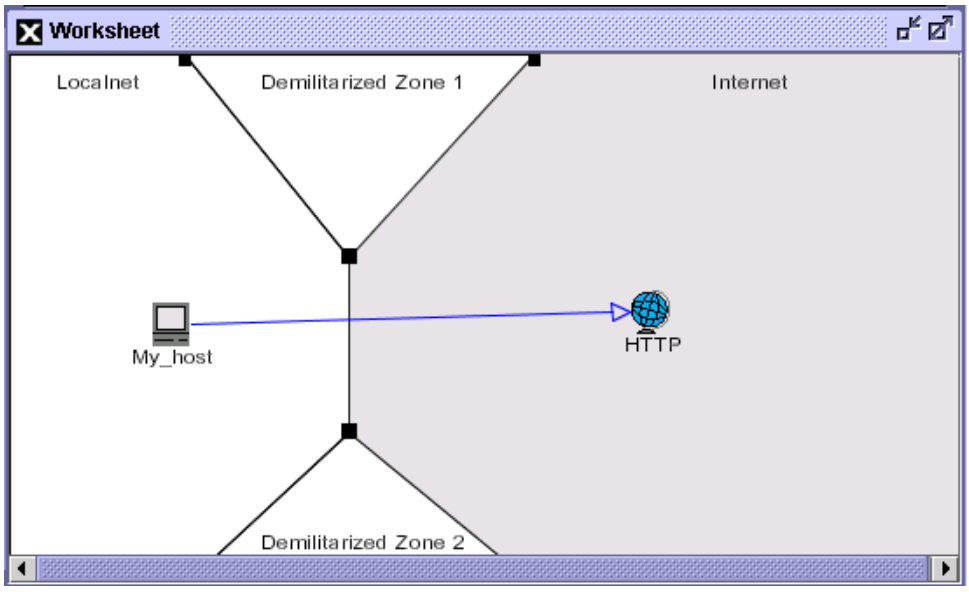


Figure 7-17 The host My_host can access all web sites on the Internet.

Example: Give the LAN access to all services on *company_server* in the DMZ.

1. Add the server *company_server* to the *DMZ*.
2. Add an ***allow*** rule from the *LAN* to the *company_server* node.

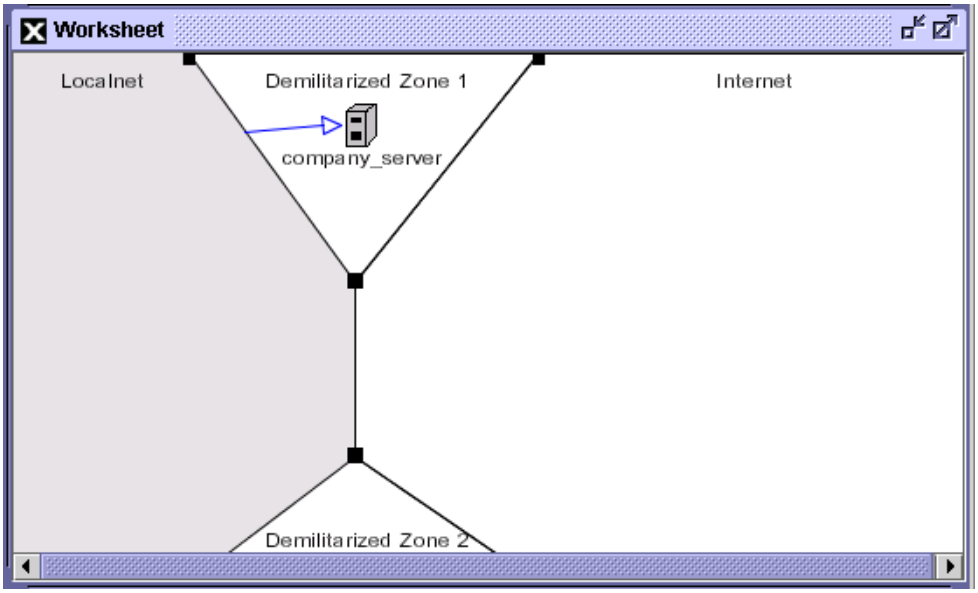


Figure 7-18 All hosts on the LAN can access *company_server* in the DMZ.

The Use of Host Folders

Example: **Prevent the LAN from accessing the computers a, b, c and d**.

1. Add the host folder *bad_hosts* to the *Internet* zone.
2. Bring up the folder's properties.
3. Add the hosts *a, b, c* and *d* to the folder.
4. Add a *deny* rule from the *LAN* to *bad_hosts*.

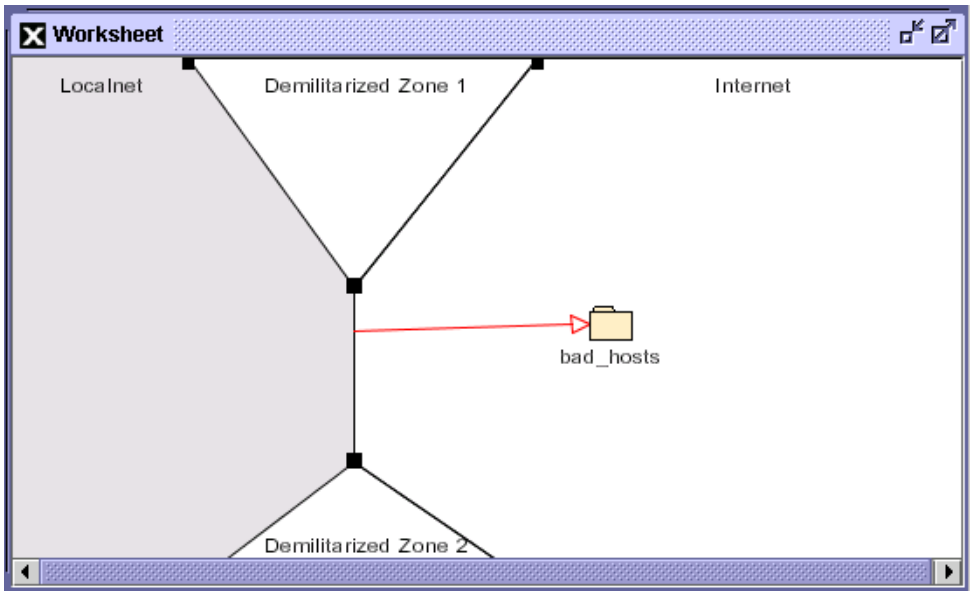


Figure 7-19 All hosts on the LAN is denied access to the hosts in the *bad_hosts* folder.

The Use of Servers

The server nodes are used for allowing/denying a source, access to *specific services on a specific host*. A server can hold one or more services.

Example: Place a public accessible web server in the DMZ. This server requires access to a DNS server on the Internet.

1. Add the server *server* to the *Demilitarized Zone 1*, with the service HTTP added.
2. Add the service *DNS* to the Internet zone.
3. Add an *allow* rule from *server* to the *Demilitarized Zone 1* in the Internet zone.
4. Add an *allow* rule from the Internet zone to server.

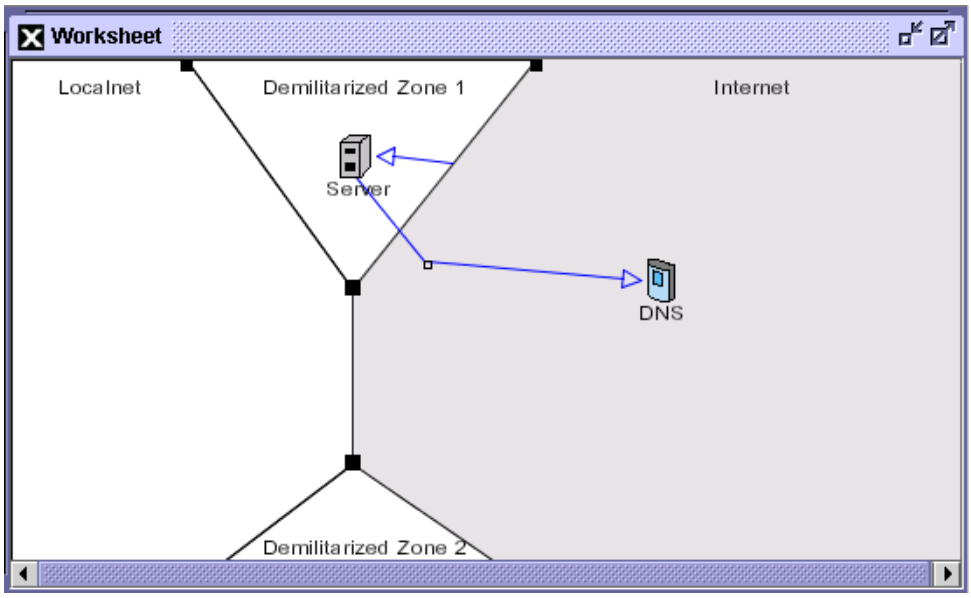


Figure 7-20 The web server *Server* is accessible from the Internet, and *Server* can access DNS servers on the Internet.

The Use of Subnets

The subnet nodes represent whole subnets. They are used for setting rules for all computers on a subnet.

Example: Deny a subnet access to the Internet.

1. Add the subnet *my_subnet* to the *LAN* zone.
2. Add a *deny* rule from *my_subnet* to the Internet zone.

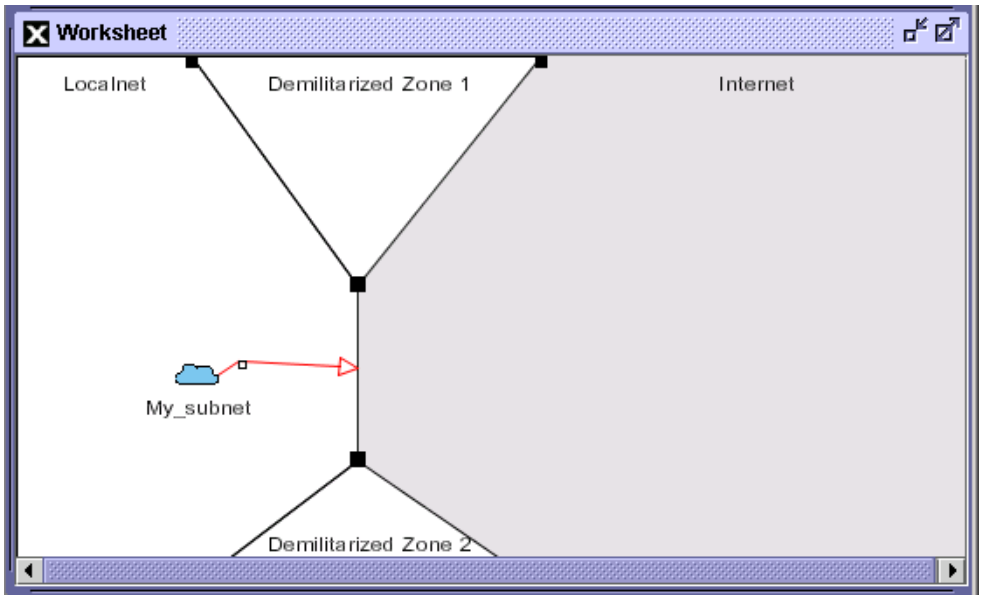


Figure 7-21 The subnet is denied access to the Internet.

The Use of Server Class

Example: Gather many servers which all provide one service, DNS, and are accessible from the LAN.

Add the server class *serv_class* to the secure zone (DMZ).

1. Add the service *DNS*.
2. Add hosts to this server class.
3. Add an allow rule from the LAN to the server class *serv_class*.

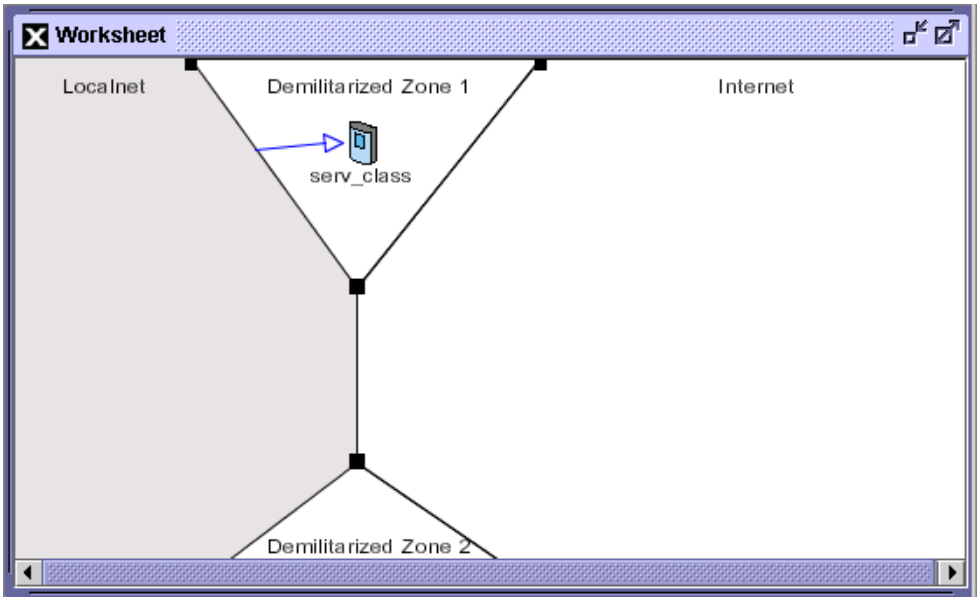


Figure 7-22 Use of server class.

The Use of Source NAT

Example: Hide the real IP address of a host in the local area network.

1. Right-click in the LAN and add the host. Enter the host properties.
2. Right-click the host and select **Source NAT** from the list.
3. Point the arrow to the Internet zone and click.

A stapled arrow now illustrates that the real IP of the host in the LAN will be replaced by the IP address of the Internet interface of the firewall. This is the default form of source NAT in the firewall, and is called *masquerading*. See Figure 7-23 on page 100.

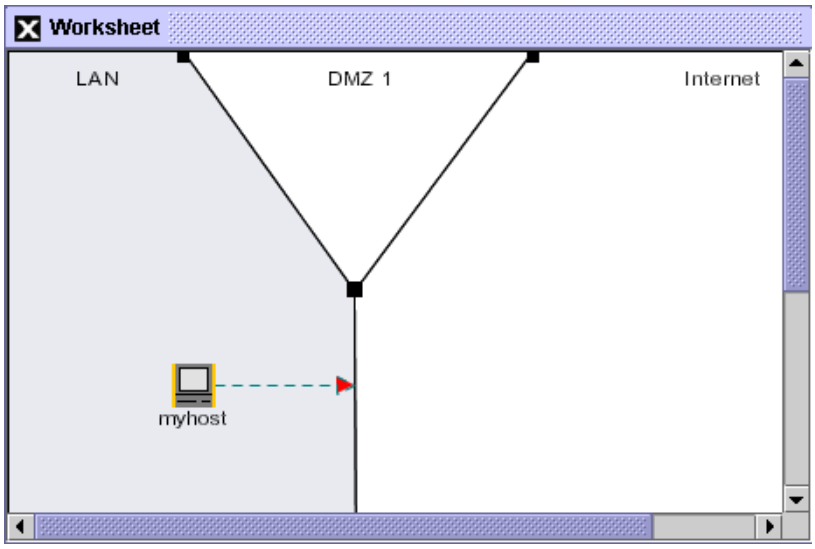


Figure 7-23 Hiding the real IP address of *myserver*.

If you would rather use another IP address than the address of the interface of the firewall as the apparent IP address of the host in the LAN, right-click on the arrow. A dialog then pops up:

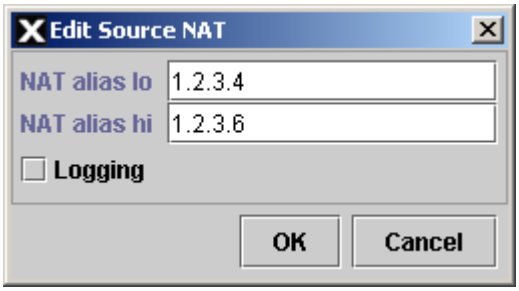


Figure 7-24 Edit Source NAT

Enter one IP alias (either lo or hi) or a range of IP aliases to be used for the host. If a range is given, the firewall will use the addresses in a round robin fashion as connections are established. The same IP address may be used for many connections at the same time.

The tip of the arrow will become red to indicate that a NAT alias has been defined.

The Use of Destination NAPT

Example: Hide port 80 on the web server running on a host in the DMZ. Also change the destination IP address of the host.

1. Right-click in the DMZ and add the host. Enter the host properties.
2. Right-click in the Internet zone, and choose **Destination NAPT**.
3. Point the arrow to the host.
4. A dialog pops up. Enter the NAT alias, e.g. 1.2.3.4, the port to forward from (80), and the port to forward to, e.g. 8080. Choose TCP as the transport protocol.

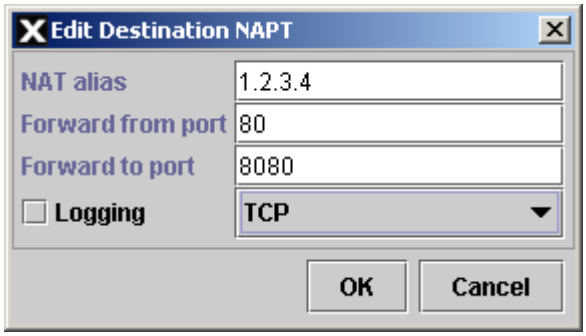


Figure 7-25 Edit Destination NAPT

Then the network address and port translation will be shown as a blue, curved arrow:

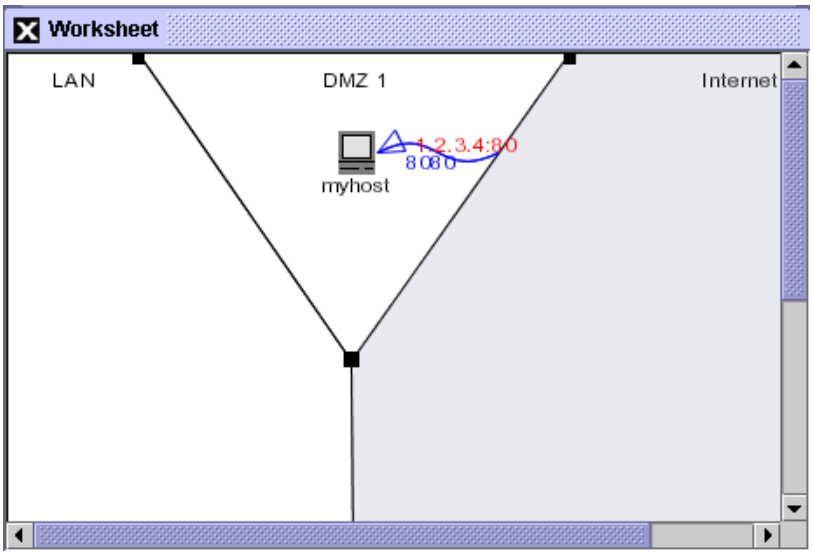


Figure 7-26 Use of destination and port address translation

The point of this example is to show how easy it is to forward web traffic from the privileged port 80 to the unprivileged port 8080. In this way you can avoid running your web server as root, which is undesirable from a security point of view. At the same time the destination address is changed, hiding the real IP address of the web sever, further improving security.

Load Balancing

Note that a destination NAPT rule also can be set up to a host folder. Then the firewall will distribute connections to the NAPT alias between all the hosts in the folder. In this way one can balance the load between e.g. several web servers.

Advanced Options

Services

The Firewall comes with the most commonly used services pre-defined. However there may be situations where services have to be manually defined. This is a complex task and should only be performed by advanced users. It is important to understand that incorrect service definitions may lead to security problems.

Services are configured in the **Services** dialog. This dialog is brought up by selecting **Application > Services**.

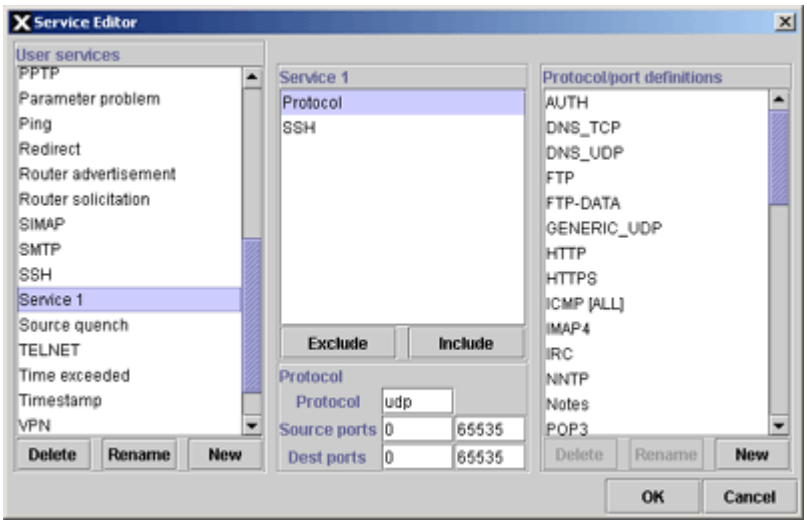


Figure 7-27 Services.

A list of all pre-defined services is available. From this dialog, it is possible to add new services, edit existing services, and delete services.

Create a New Service

Clicking **New** in the services dialog will create a new service and open the 'Add user service' box below.

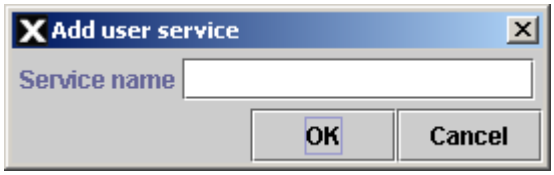


Figure 7-28 Create new service.

Enter a name for the new service. This name should identify the service in a unique way.

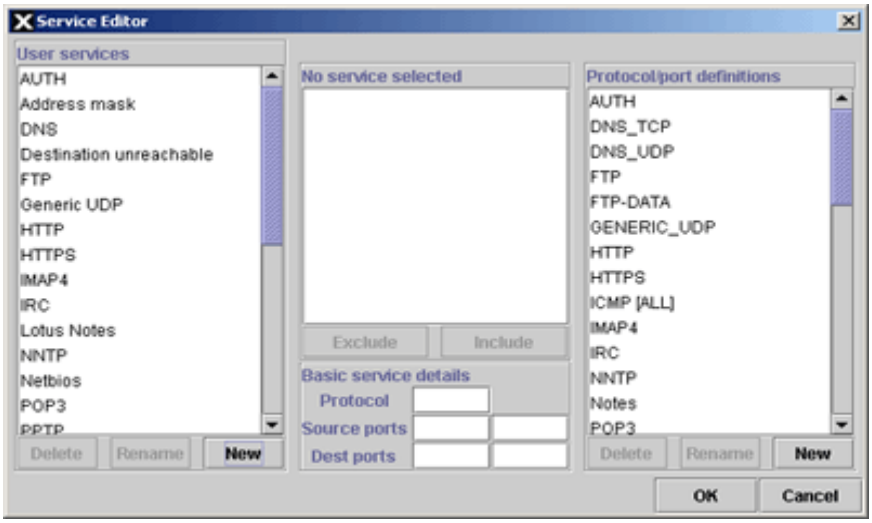


Figure 7-29 Service Editor.

Creating a New Protocol/Port Specification

If a specification needed does not exist, create a new protocol/port specification by clicking **New**. Enter a name for the new protocol/port specification.

Figure 7-30 Create new protocol/port specification.

Select type of protocol. Clicking in the Protocol box will provide a list.

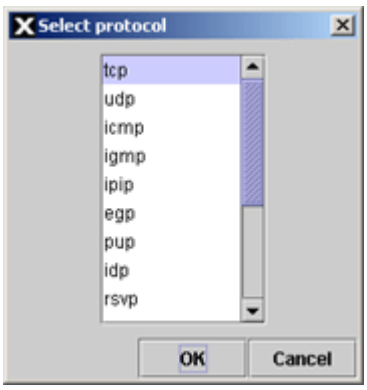


Figure 7-31 Select protocol.

Enter the source port range. The sources will contact the services from these port numbers. If only one port is used, this port number has to be inserted as both start and end ports.

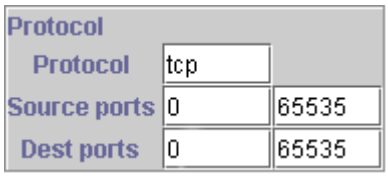


Figure 7-32 Set source port range.

Enter the destination port range. These are the port numbers where the service can be contacted. If only one port is used, this port number has to be inserted as both start and end ports.

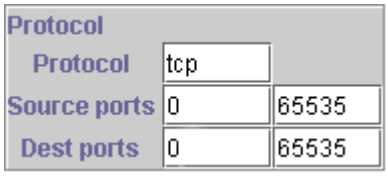


Figure 7-33 Set destination port range.

Select if the traffic should be bidirectional. TCP services have to be bidirectional.

Figure 7-34 Assign Protocol/Port to Service.

Add the created port specification by clicking **Finish**.

Editing an Existing Service

Only those services you have added can be edited.To edit an added service select **Application > Services**. In the services dialog select the service you want to edit, the editable fields are now available. Please note that when editing services, all entities using these services in the worksheet must be reinserted. The changes made to the service definitions do not propagate to the worksheet.

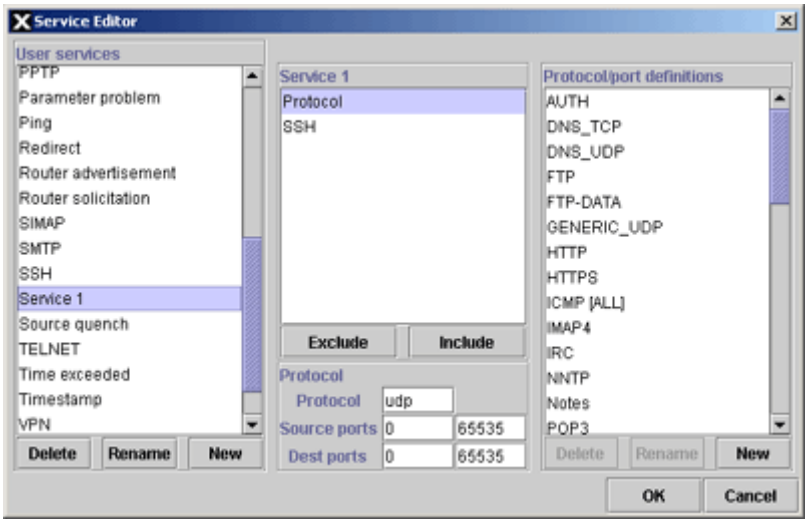


Figure 7-35 Edit service properties.

LAN Client Configuration

After the Firewall has been installed and configured, the network configuration for all computers on the LAN may need to be reconfigured. This is because the firewall is now the new gateway of the LAN.

Hint: If the IP address of the firewall on the LAN is the same as the old gateway, and there has been no restructuring of the addresses on the LAN, the computers do not need to be reconfigured.

MS Windows 95/98

Bring up the network settings (Figure 6-36) by selecting **Start > Settings > Control Panel > Network.**

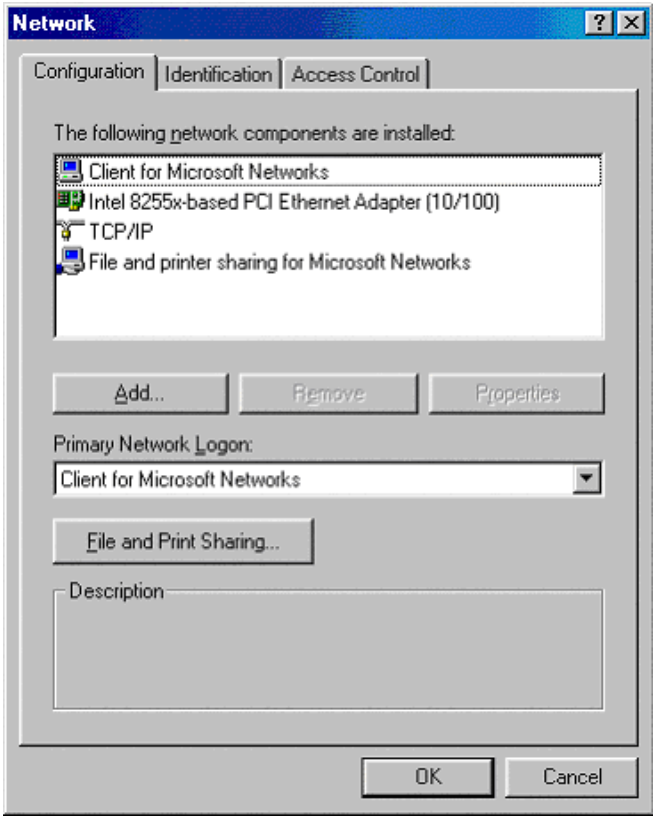


Figure 7-36 Network properties.

Select **TCP/IP**, and then click **Properties**. The TCP/IP dialog appears.

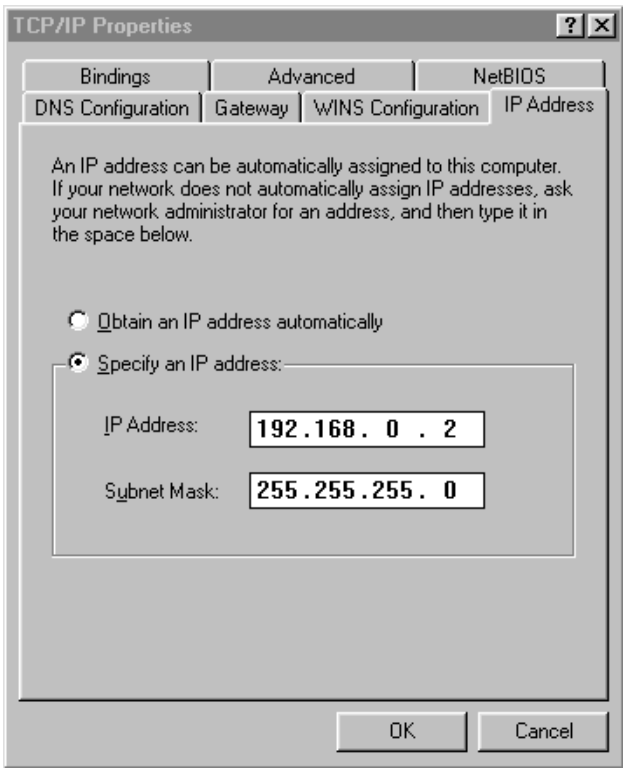


Figure 7-37 TCP/IP properties.

Select **IP Address** if not already selected. If the IP address or Subnet mask have changed, enter the new values here.

Select **Gateway** and remove the old gateway by selecting in the list, then click on **Remove**. Add the IP address the firewall was designated on the LAN in the **New Gateway** field. Click **Add**. Finish the update by clicking **Ok**.

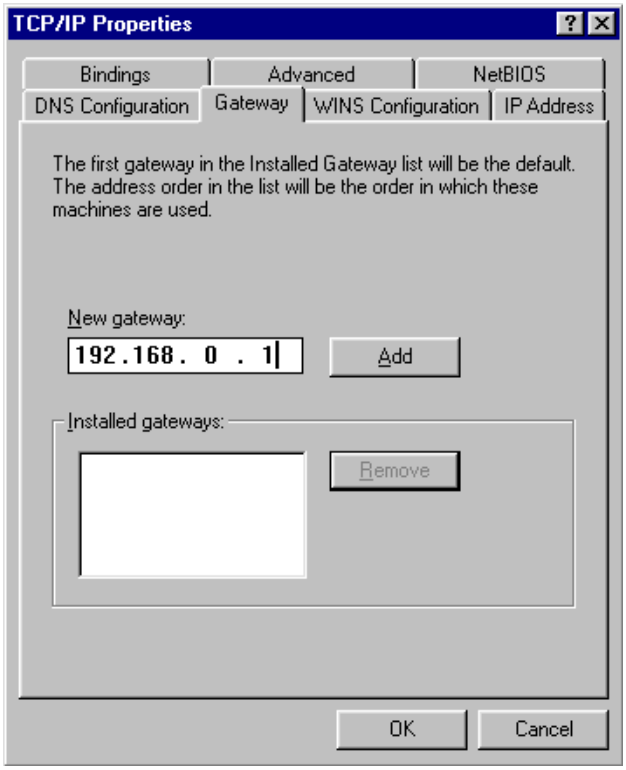


Figure 7-38 Gateway properties.

Windows will now perform a reboot. When the operating system has come up again, network configuration should function properly.

MS Windows NT 4.0

Bring up the network dialog by selecting **Control Panel > Network**.

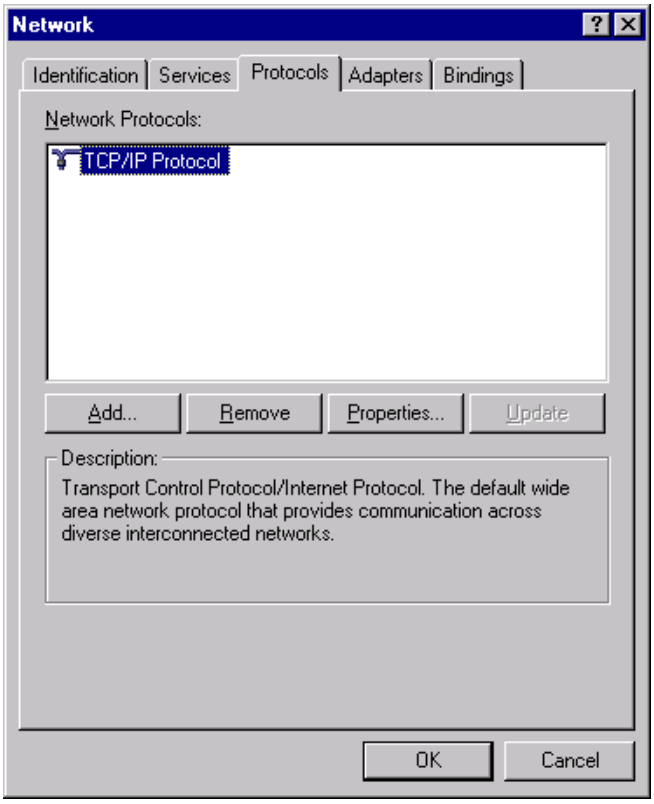


Figure 7-39 Network properties.

Choose the tab **Protocols** and select TCP/IP protocol from the list of protocols and click **Properties** to bring up the TCP/IP dialog. (Figure 7-41)

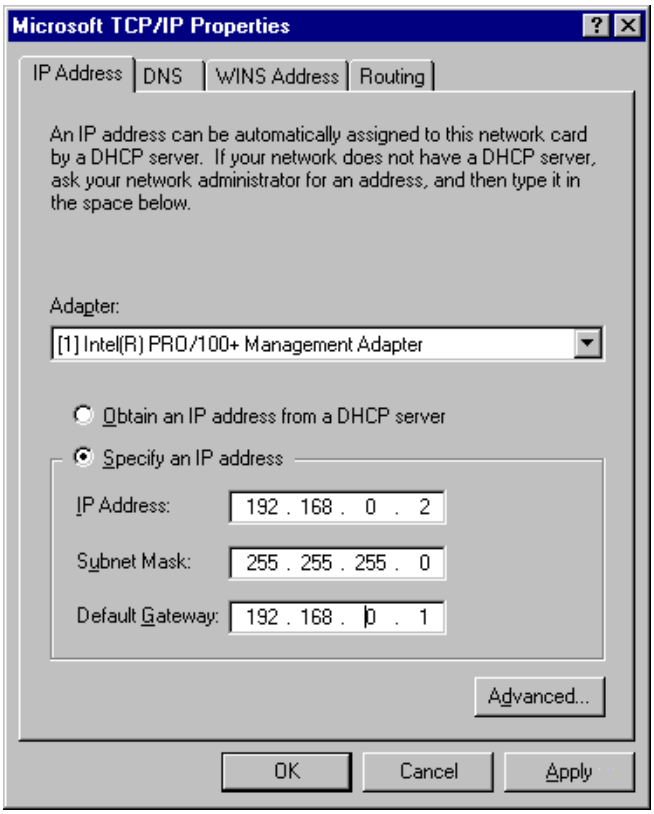

Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[1] Intel(R) PRO/100+ Management Adapter
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
192 . 168 . 0 . 2
Subnet Mask:
255 . 255 . 255 . 0
Default Gateway:
192 . 168 . 0 . 1
Advanced...
OK
Cancel
Apply

Figure 7-40 TCP/IP properties.

Select the network interface card connected to the LAN from the list of Adapters. Change the **IP Address** and **Subnet Mask** if necessary. Change the value **Default Gateway** to the firewall's IP address on the LAN. Save settings by clicking **OK**.

MS Windows 2000

Bring up the network dialog by selecting **Control Panel > Network and Dial-up Connections**. Select **Local Area Connection** and click the **Properties** button.

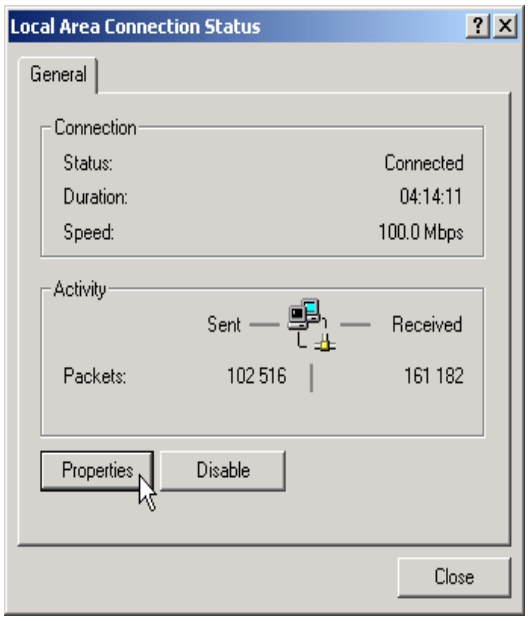


Figure 7-41 Local area connection.

The dialog Local Area Connection Properties dialog opens. Select the **General** tab and select the network interface card connected to the LAN from the list of Adapters. In the component list highlight **Internet Protocol (TCP/IP)**. Click **Properties**.

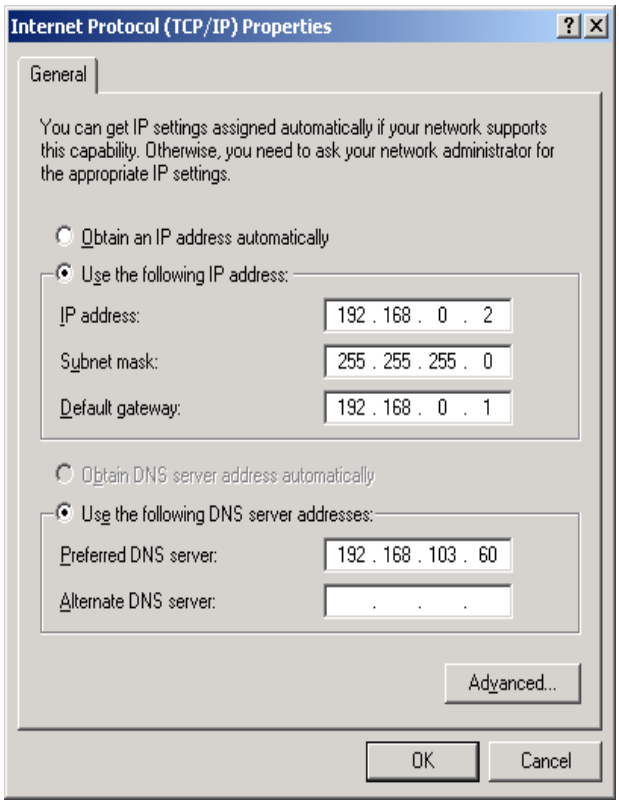

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
192 . 168 . 103 . 60
Alternate DNS server:
Advanced...
OK
Cancel

Figure 7-42 Windows 2000, TCP(IP properties.

Change the **IP Address** and **Subnet Mask** if necessary. Change the value **Default Gateway** to the firewall's IP address on the LAN. Save settings by clicking **OK**.

Linux

Change the IP address of the computer if necessary. Set the gateway address to the firewall's IP address on the LAN. Use a network configuration tool, or edit `/etc/sysconfig/network-scripts/ifcfg-eth0` manually.

Trustix™

Appendix A

Firewall Rules and Policy

Whenever you configure the firewall by drawing arrows between zones, hosts, services and other entities, it is translated into firewall rules. These rules have a structure that makes the firewall safe to use, even if the user makes some mistakes or misunderstands the network infrastructure or routing.

The source and destination of the rule is the most important factor when deciding the priority of the rules:

1. Host (server, host, serverclasses)
2. Network (subnet, zone)

This means that a host (which is more specific than a network) has the highest priority with regards to zones and subnet. A subnet within the same IP-range as the network it is located within has a higher priority than the zone.

The priority of the rule is based on the type of rule. These are, in order of importance:

1. Destination Network Address Translation
2. Deny
3. Allow
4. Source Network Address Translation

This means that you can specify Deny between all of your zones and still be able to specify Allow or Source NAT for specific hosts within those networks.

Trustix™

Appendix B

Using ssh in MS Windows

SSH (Secure Shell) is a remote terminal application which is used to connect to many terminal / Unix servers. Microsoft Windows does not include any ssh client software, so we provide an easy to use ssh client called putty ssh. This application can be run directly from the CD-ROM and is installed with the firewall client application into the folder at:

<drive>:\Program Files\Comodo Trustix\Firewall 4\thirdparty\PuTTY.

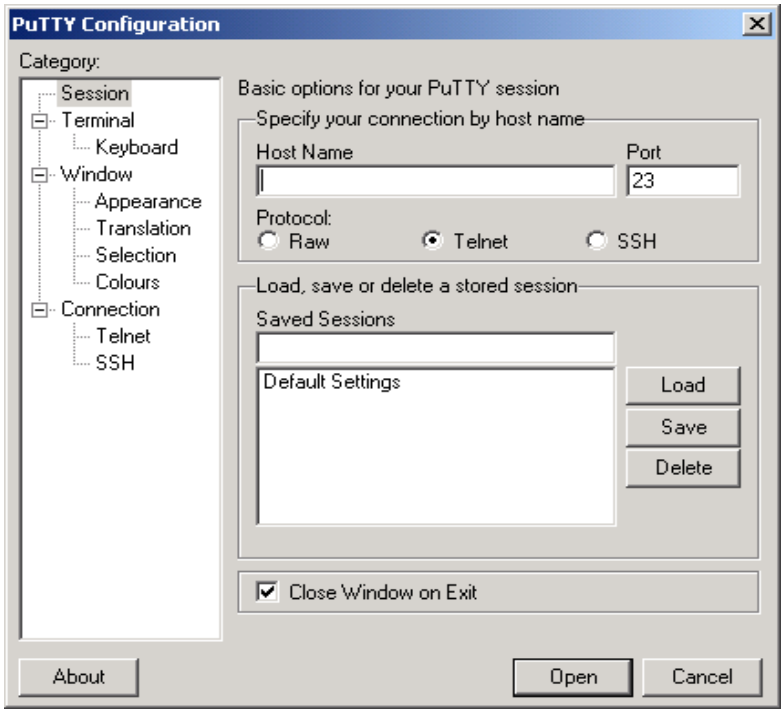


Figure B-1 Putty configuration.

To connect to your firewall, you must use port 350. This is to avoid any confusion with regular ssh servers and port forwarding done by the firewall.

The procedure below shows how to get started using putty ssh.

1. Start putty by double-clicking the putty application from Windows Explorer. The application is found on the Comodo Trustix firewall CD-ROM.
2. Enter the hostname or IP address of the firewall. An example: myfirewall.mycompany.com or the numeric representation of this hostname: 10.0.0.1
3. Select SSH as the **Protocol**, and then Enter the value 350 in the **Port** field.
4. Click **Open** and you are presented with a new window where you must authenticate to the firewall.
5. Enter the username “root” and your system password (which you have already configured on the console).

You are now ready to use putty ssh.

Trustix™

Appendix C

Predefined Services

The following services are predefined in the Firewall.

AUTH

The Authentication Server Protocol. Service for determining the identity of a user of a particular TCP connection.

Address mask

A bit mask used to identify which bits in an IP address correspond to the network address and subnet portions of the address.

Destination Unreachable

An indication from a host that a packet you sent did not reach its destination.

DNS

The Domain Name System. A distributed database used to map IP addresses to hostnames.

FTP

File Transfer Protocol. Only active FTP through masquerading is supported due to security.

Generic UDP

Allows general UDP (User Datagram Protocol) traffic. Provides simple datagram services. If you want to enable complete access to the Internet, add an allow rule to a UDP service, as normal rules only include TCP traffic.

Note: Setting an allow rule from your LAN to UDP on the Internet, opens your network to hostile scanning, as UDP allows bidirectional traffic!

HTTP

The World Wide Web.

HTTPS

Encrypted web. HTTPS is a protocol, which provides HTTP over an SSL encrypted socket.

IRC

Internet Relay Chat used for On-line chatting.

Lotus Notes

Lotus groupware product, use this service.

Netbios

A set of network commands that the application program uses in order to send and receive data to another computer on the network. MS Windows 2000 hosts use Windows directory Service.

NNTP

Network News Transfer Protocol. Provides access to Usenet news groups.

POP3

Post Office Protocol version 3. Used for retrieving electronic mail from a server.

PPTP

Point-to-point Tunneling Protocol. Used to create a VPN between MS Windows NT computers.

Ping

Packet InterNet Groper. Used to establish whether there is contact between networked computers.

IMAP4

Internet Message Access Protocol version 4. Used for accessing electronic mail on a server from a client.

SIMAP

Secure IMAP. Used for accessing electronic mail on a server from a client, through an encrypted connection.

SMTP

Simple Mail Transfer Protocol. Used for transferring electronic mail between mail servers.

SSH

Secure Shell. Service for logging into a UNIX computer through an encrypted connection.

TELNET

Service for connecting to a remote machine.

VPN

The use of encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

Windows Directory Service

Microsoft Windows Active Directory.

Windows Networking
Microsoft Windows support for sharing file and print services.

The following services are less commonly used. Trustix suggest only advanced users implement these.

Parameter problem

Unspecified problem, this may be an indication of an attack on your firewall.

Redirect

This may be an indication of an attack on your firewall by redirecting your traffic.

Router advertisement

ICMP router discovery message. The router periodically multicasts a router advertisement from each of its multicast interfaces, announcing the IP address (es) of that (those) interface (es).

(Source: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1256.html)

Router solicitation

ICMP router discovery message. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive.

(Source: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1256.html)

Source quench

Indication of congestion on the Internet.

Time exceeded

When sending fragmented IP datagrams, the sender of this message never received all the fragments.

Timestamp

Generally used to identify object creation, modification, last access times etc. Also used to identify an event in event or error type logs.

Services and Port Ranges

The following table gives an overview of the predefined services in the Firewall, specifying their port number ranges.

Table C-1 Port ranges.

Service	Protocol	Source port range	Destination port range
AUTH	TCP	all	113/113
Address mask	ICMP	17/17	all
DNS	TCP	all	53/53
	UDP	all	53/53
Destination unreachable	ICMP	3/3	all
FTP	TCP	1024/65535	21/21
	TCP	1024/65535	20/20
Generic UDP	UDP	all	all
HTTP	TCP	1024/65535	80/80
HTTPS	TCP	1024/65535	443/443
IMAP4	TCP	1024/65535	143/143

Table C-1 Port ranges.

Service	Protocol	Source port range	Destination port range
IRC	TCP	1024/65535	6667/6667
Lotus Notes	TCP	1024/65535	1352/1352
NNTP	TCP	1024/65535	119/119
Netbios	TCP	all	137/139
	UDP	all	137/139
POP3	POP3	1024/65535	110/110
PPTP	TCP	1024/65535	1723/1723
	TCP	all	all
Parameter problem	ICMP	12/12	all
Ping	ICMP	8/8	all
Redirect	ICMP	5/5	all
Router advertisement	ICMP	9/9	all
Router solicitation	ICMP	10/10	all
SIMAP	TCP	1024/65535	993/993
SMTP	TCP	1024/65535	25/25
SSH	TCP	all	22/22
Source quench	ICMP	4/4	all
TELNET	TCP	1024/65535	23/23
Time exceeded	ICMP	11/11	all
Timestamp	ICMP	13/13	all
VPN	UDP	500/500	500/500
	TCP	all	all
	TCP	all	all
Windows Directory Service	TCP	all	445/445
	UDP	all	445/445

Table C-1 Port ranges.

Service	Protocol	Source port range	Destination port range
Windows Networking	TCP	all	137/139
	UDP	all	137/139
	TCP	all	445/445
	UDP	all	445/445

Trustix™

Appendix D

Upgrading the Firewall

The Firewall software is upgradeable through the Firewall Upgrade System. Since your firewall is always connected to the network, you can activate firewall server upgrades by accessing the firewall console and select upgrade.

Security when Upgrading

To maintain security when upgrading, the upgraded software is checked for integrity, author and place of download. The only valid downloads are those signed by the Comodo Trustix Enterprise Firewall team and authenticity is insured by using *gpg*, a version of *pgp security*.

How to Upgrade

Firewall upgrades are announced to customers through e-mail, or other notifications specified upon purchase. The customer will then have to access the firewall console and initiate the upgrade.

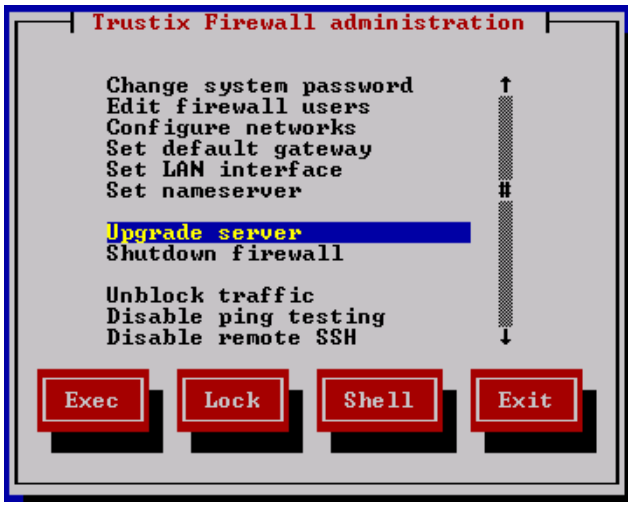


Figure D-1 Main menu - upgrade server.

Access to the upgrade-server is then granted from the firewall and software will be downloaded as fit for your version of the firewall.

Preparations before Upgrade

Upgrade preparations should include making sure that your ISP will not do maintenance on your leased lines. Upgrades will be retrieved from Comodo Trustix Distribution Servers.

Before an upgrade is initiated, a confirmation is required to make sure that all preparations are done.

Trustix™

Appendix E

Console Tools on the Firewall

The firewall has some console-tools included for the advanced user, who would like more in depth views of the firewall. The console tools are not required or necessary to operate the firewall, and access to the console is mandatory to use these tools.

Log into the console using the Shell feature on the firewall console, or use ssh to access the firewall (see "Using ssh in MS Windows," on page 115).

fwlogwatch

The fwlogwatch-tool is an open source tool written by Boris Wesslowski and operates on the logs generated by the firewall. To be able to use the utility, you must first enable logging in the firewall client.

The manual page of fwlogwatch describes the utility like this:

fwlogwatch produces ipchains, netfilter/iptables, ipfilter and cisco log summary reports in text and HTML form and has a lot of options to find and display relevant patterns in packet logs. With the data found it can produce customizable incident reports from a template and send them to abuse contacts at offending sites or CERT coordination centers. Finally, it can also run as daemon and report anomalies or start countermeasures.

The manual page of fwlogwatch also includes an example of how to use the utility like a specified report-generation utility.

If you want a HTML summary 'log.html' of all packet filter entries at most one day old representing at least two connection attempts logged to the file 'messages' with output including timestamps, time intervals, resolved IP addresses and service names and with connections separated by protocol, source and destination ports and TCP options you would use fwlogwatch -s -d -t -z -y -n -p -w -l 1d -m 2 -o log.html -f messages

Trustix™

Appendix F

VPN and Road Warriors

Virtual Private Network

http://www.whatis.com defines VPN as follows:

"A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company.

The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A virtual private network makes it possible to have the same secure sharing of public resources for data. Companies today are looking at using a private virtual network for both extranet and wide-area intranet.

Using a virtual private network involves encrypting data before sending it through the public network and decrypting it at the receiving end. [...] VPN software is typically installed as part of a company's firewall server."

Digital Certificates

http://www.whatis.com defines "Digital Certificates" as follows:

"A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web.

It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encryption messages and digital signature), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real."

The Trustix Firewall acts as its own CA. If you intend to create Certificate authenticated VPN connections, you will need to create a CA certificate for the built-in Certification Authority module of the firewall. If you intend to create VPN connections between several Trustix Firewalls in your network, you should in advance designate one of these firewall servers as the company's VPN CA, and only issue certificates from this server. For the other firewall servers this means that instead of issuing their own certificates, they will import all certificate information necessary from the designated CA server.

In practice, what any Trustix Firewall acting as a VPN gateway needs, is to import the public part of the CA certificate of the company's VPN CA, both the public and private parts of this firewall server's identification certificate, and the public parts of the certificates other entities will use when trying to establish a VPN connection with this server.

Both in this documentation and in the Trustix Firewall product, we talk about three 'kinds' of certificates:

- Client certificates are the certificates others use to identify themselves to the Trustix Firewall when trying to establish a VPN connection. The firewall server only needs to know the public parts of these certificates.
- The server certificate is the certificate the Trustix Firewall server uses to identify itself to others during the VPN connection negotiations. The server needs to know both the public and private parts of this certificate.

  Technically there is no difference between client and server certificates, so they are collected in the 'User certificates' group in the built-in CA module.

  Note that you need to explicitly tell the VPN subsystem which user certificate to use as its identifying server certificate by clicking on the 'Use as ID' button in the User Certificates dialog in the firewall client.
- The CA certificate is the certificate that the company's VPN CA uses to sign any user certificate it issues. It is possible to use this certificate as the VPN CA's identification certificate, but we do not recommend this.

From the CA module's VPN Certificates menus in the firewall client, you have access to all the functionality needed to create certificates and to export and import public and private parts of the user certificates. (You may only export the public parts of the VPN CA certificate).

The process of creating certificates is described later in this appendix.

Road Warriors

The connecting 3rd party client is called *Road Warrior*. This definition is used to describe a person who changes their IP address most of the time (due to local dial-up connections and dynamic IP allocation).

Road Warriors often need to access their company's internal network, or some other designated part of the network to retrieve or share documents, presentations and other information. Because of the nature of the Road Warrior, it is not possible to use static IP addresses to allow their VPN connections. To identify the Road Warrior and allow his incoming VPN connections, the Firewall use digital certificates for verification of the connecting party.

Considerations when Allowing Road Warriors

Road Warrior functionality in a firewall is a good thing, although the security administrator must keep a few things in mind when allowing this functionality on the firewall:

- The network
- The pass phrase
- The Road Warrior's computer
- Managing the certificates

The Network

By allowing VPN connections in general, and Road Warriors in particular, you have an opening in your firewall. This opening is protected on both sides (by the firewall and the Road Warrior) so care has to be taken to secure both of these sides.

It is also important that you protect your internal network and create a separate secure zone where you want your Road Warriors to gain access.

You are better off defining a fourth (or third) firewall zone which is cut off from the rest of your network, where Road Warriors can access limited-access file servers, mail servers or other company-required services.

The Pass Phrase

The *pass phrase* is the key to unlock the Road Warriors digital certificate. If this pass phrase is too easy to guess, a possible attacker will be able to gain access to your internal network.

Good pass phrases are typically long (above 12 characters) and contain a mix of upper case and lower-case characters with some additional special characters (examples of special characters include: "!","@","$","%" and more).

The most used method of breaking a pass phrase is to apply brute-force attacks, by e.g. using a mix of dictionary words, so be aware that dictionary-based words ("book", "chair", "mom", etc) should not be used.

The last thing to remember is that social engineering is the best way to break a pass phrase. Do not use your date of birth, the current age of your dog, your social security number or other kinds of personal information in your pass phrase. This only makes it easier for others to gain access to your digital certificate (and then, your corporate network). With that said, keeping the certificate stored in a secure place is also a good idea, and the best way to avoid compromise.

The Road Warrior's Computer

After a Road Warrior establishes a connection to the company Firewall, he gains access to proprietary information or confidential documents that are not meant for distribution.

If someone was able to gain access to the Road warrior's computer and look at his files, or even worse: use the computer's network connections, access to the corporate network is an inch away. Securing the Road Warrior's computer is as important as securing your internal network. This is potentially a large problem, since Road Warriors can operate on different Operating Systems.

Always updating your OS and software is the first and most important thing to have in mind. Using 3rd-party tools for securing your desktop is also advisable.

Managing the Certificates

The security administrator is responsible for managing the issued certificates. The creation and storage is done by the Firewall, but revoking unused or invalid certificates is just as important.

If a user leaves his assignment (as a Road Warrior), he must have his certificate revoked. This is to make sure that this person will not be able to access the company network again.

Using Road Warrior Functionality in the Firewall

This section explains what you have to do in order to manage your Road Warriors and the certificates:

- Creating certificates
- Connecting to a firewall
- Revoke certificates

Creating Certificates

The Trustix Firewall has a built-in 'mini-CA', which is accessible from the Firewall Client through the **Firewall > VPN Certificates** menu.

The first thing you will need to do, is to create a CA certificate. This certificate is used to sign all subsequent user certificates that you create.

CA certificates are created through the menu **Firewall > VPN Certificates > CA Certificates**. This opens a dialog containing a list of the currently known CA certificates. Clicking **Create** brings up the certificate details dialog. See Figure F-1 on page 131

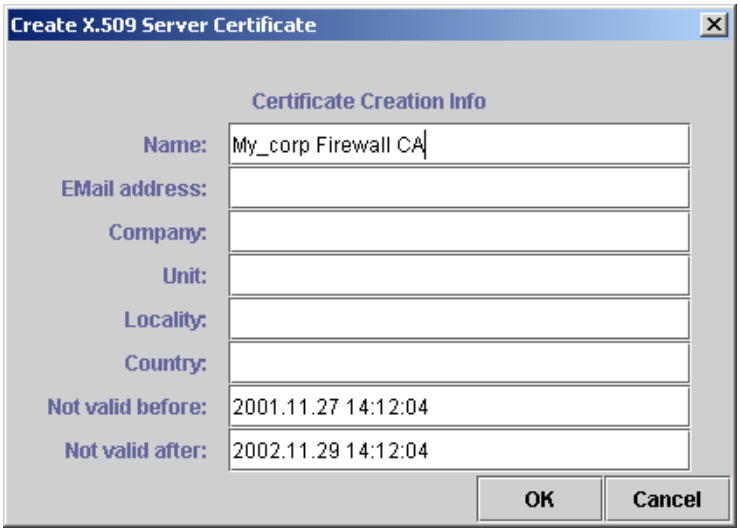


Figure F-1 Create server certificate.

In this dialog you fill in the data for the CA certificate. All fields except **Name**, **Not valid before** and **Not valid after**, are optional. If you choose to fill in the **Country** field, please note that this field must contain a two-lettered upper-case country code (NO for Norway, US for United States of America, etc). This is the only format the CA will accept for this field.

If the clocks on the server and client hosts are not synchronized, there may be a delay before the certificate is validated. If you wish to avoid this, backdate the **Not valid before** a day or two.

When you are satisfied with the entered information, click **OK**, and the new certificate will appear in the list of known CA certificates.

In the **CA Certificates** menu you may export a CA certificate by clicking **Export**. This will export the public parts of the highlighted certificate to a file. This, and other CA certificates, may be imported by clicking **Import**. Note that you may not use an imported CA certificate as a signer certificate when you create user certificates, as only the public parts were imported, and the CA needs the private parts for signing.

Each Trustix Firewall acting as a VPN gateway should have its own user certificate - the 'server' certificate. Select **Firewall > VPN Certificates > User certificates** to display the list of user certificates currently known to the server.

Creating a user certificate is practically identical to creating a CA certificate, the only difference is that in the Create User Certificates dialog there will be a drop-down selector above the information entry fields where you select which CA certificate you want to use for signing the user certificate. See Figure F-2.

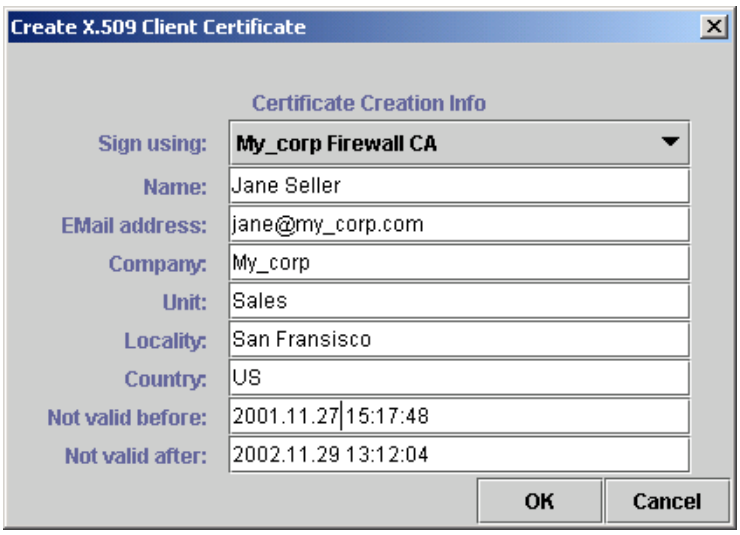


Figure F-2 Create client certificate.

When you have created the certificate, highlight it in the list in the **User Certificates** dialog, and click **Set as ID**.

Note: *If you have designated another Trustix Firewall as your company's VPN CA, the server certificate must be created on that firewall instead. Export the VPN CA's CA certificate, and then export the user certificate as a PKCS12 bundle. (This is the only way to export the private parts of a certificate, and you are asked for a password to encrypt the data before exporting).*

Import the exported CA certificate from the **CA Certificates** dialog window, and the server certificate from the **User Certificates** dialog, of the server that should use this server certificate, and **Set as ID** as above.

Each remote VPN endpoint needs one certificate. This implies that you may need to create additional user certificates - client certificates - for these endpoints. The process of creating such certificates is identical to creating server certificates, except that you must not **Set as ID** these certificates.

Each client certificate must be exported as a PKCS12 bundle from the Trustix Firewall (or the company's designated VPN CA, if you have one). In addition the client will normally need the public parts of the company's VPN CA certificate (exported as described above), and either the public parts of the server certificate of the Trustix Firewall VPN gateway it will connect to (exported as a client certificate, but answer no when asked whether to export as PKCS12), or the exact spelling of the information fields of the server certificate.

To see the information the server certificate contains, highlight the certificate in the dialog list box, and click **Details**. The names of the fields may vary between different VPN software, but it should not be difficult to see what is what.

Now you are ready to use third party software to connect to the firewall via a VPN tunnel. The Trustix Firewall supports PGPNet™ and VPN client software based on the Safenet distribution. Among the latter we have tested Netsceen-Remote™. The Trustix Firewall also supports the built-in IPSec clients in Microsoft Windows 2000 and XP.

For more information, see: `http://www.trustix.com`

Connecting to a Firewall

Licence

First, you have to have a Road Warrior license for your firewall. Ensure that you have bought and enabled the license (see "First-time Configuration of Firewall," on page 41). If you require a new license for your firewall, contact Trustix Sales on:

sales@trustix.com

Using Digital Certificates

To authenticate as a road warrior, you must have an x.509 digital certificate. This certificate is personal for every road warrior and the generated password / pass phrase must be kept secure.

To create a digital certificate (packed as a pkcs12 bundle from the firewall), access the Firewall menu in the administration client and select VPN.

Adding Road Warriors to the Worksheet

To add a Road Warrior, perform the following procedure:

1. Right click in the Internet-zone of the worksheet, and select the **Road Warrior** item. This opens the VPN Road Warrior Setup dialog.

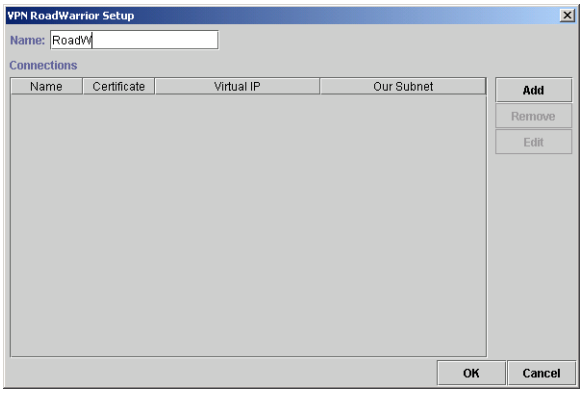


Figure F-3 Road Warrior setup.

2. Enter the name you wish to use for the node in the **Name** field. Click **Add** to open the Add Road Warrior Connection dialog.

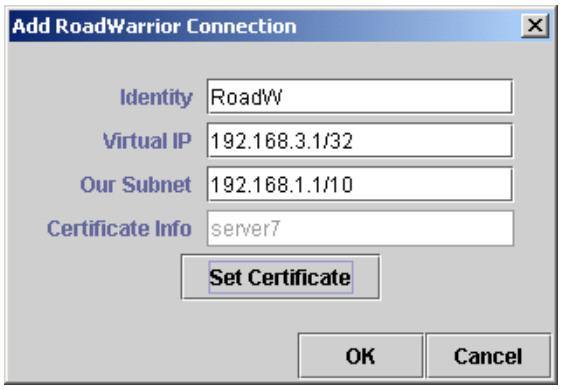


Figure F-4 Road Warrior connection.

3 Fill in the required fields:

a Identity - Type a unique identifier for the connection.

b Virtual IP (Optional) - This is the IP address the roadwarrior uses for all 'user' traffic through the VPN tunnel. If this address is given, it must be given with a trailing /32. The address must be provided to the roadwarrior by the IT staff, and it corresponds with the 'Virtual IP' field in the NSRemote client.

c Our Subnet - The IP range that you wish to allow access to through the VPN tunnel. If this field is left blank, by default the tunnel reaches the zone where the tunnel arrow ends.

d Certificate info - This field shows information on the selected certificate. Select which certificate to use by pressing the **Set Certificate** button.

4 Click OK in the Add Road Warrior Connection dialog to add the connection, and OK in the VPN Road Warrior Setup dialog. The new node is now represented by an icon in the Internet zone of your GUI.

5 Add a VPN tunnel by right-clicking in the (LAN) zone where you want the VPN tunnel to start. This produces an arrow that you drag and set by clicking on the icon representing your new roadwarrior.

Figure F-5 Activate VPN tunnel.

Activate the VPN tunnel by right-clicking on the arrow. Then select **Activate**.

Revoking Certificates

To deny access to a road warrior user, which already has access to the firewall, you must revoke his certificate on the server-side.

Use the **Firewall > VPN Certificates > User certificates** menu and highlight the certificates that you'd like removed, and then click **revoke**. These certificates are no longer active. If you decide to reactivate them again, go to the **Firewall > VPN Certificates > Revoked certificates** menu. This dialog provides a list over all revoked certificates. Select the certificate you wish to reactivate and click the **Recall** button.

Available third-party VPN clients

To view optional third-party IPSec VPN clients available, go to the Trustix website at www.trustix.com and select "Technical Services" from the menu. Here you will find documents describing how to use third-party VPN software.

Interoperability

The VPN functionality in the Trustix Firewall server has been implemented with FreeS/WAN. To see an updated list of which other firewalls are compatible with IPSec and thus the Trustix Firewall, look for the interoperability chart on the FreeS/WAN home page at:

`http://www.freeswan.org`

Trustix™

Appendix G

Virtual LAN

Concept

XSentry 4.1 enables the creation of Virtual LANs on the server, allowing to have many logical Local Area Networks within the same physical network by assigning more than one IP address to the same physical interface using the virtual interfaces concept. These logical Local Area Networks interfaces will operate independently of each other as they are placed in different physical LANs.

Virtual LAN's can be added, modified or deleted from both the XSentry client or the xsadm console.

Client Side Virtual LAN - java client

In this version VLANs can be added, modified and removed from the Java Client. There is a new menu VLAN added which has three menu items Add VLAN, Modify VLAN, and Remove VLAN. Selecting Add VLAN will bring one dialog which takes all the necessary information to create a VLAN. Any VLAN can be removed by selecting 'remove VLAN' and can be modified using 'modify VLAN'.

The VLAN menu consists of:

- Add VLAN
- Modify VLAN
- Remove VLAN

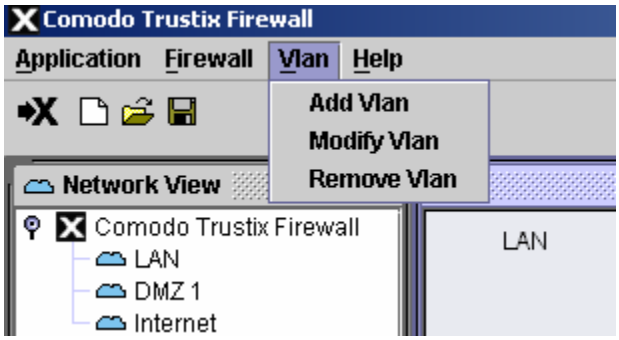


Figure G-1 VLAN

Add VLAN

Selecting 'Add VLAN' prompts the user to enter information about the new virtual LAN in the dialog below. Click 'OK' to create the new vlan.

Figure G-2 Add VLan

The newly added VLANs will be shown in the Worksheet view and the Tree view, as shown below.

Modify VLAN

Selecting 'Modify VLAN' leads to a dialog box displaying all available VLANs. Select the VLAN whose settings you wish to alter.

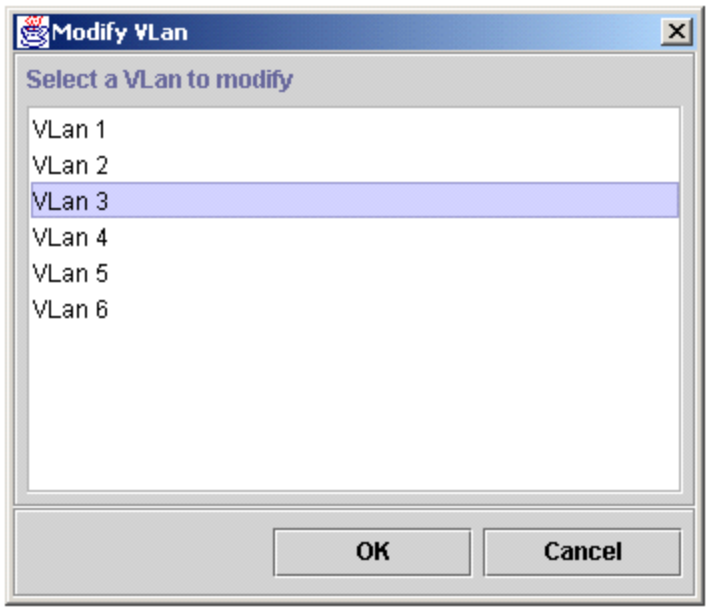


Figure G-3 Modify VLan

After choosing the particular LAN, click 'OK'. You will then be able to modify the properties of the VLAN as shown below.

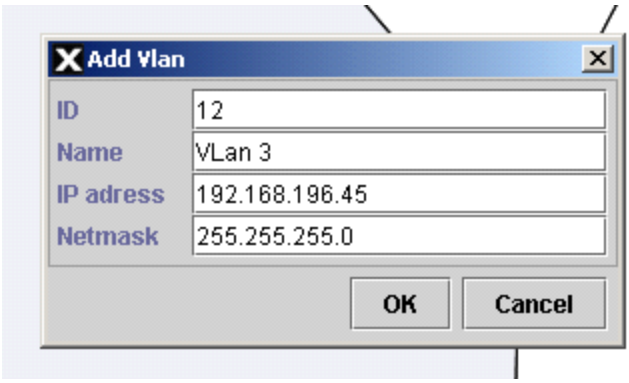


Figure G-4 Add Vlan

Remove VLAN

Similarly to the 'Add VLAN', the 'Remove VLAN' option lists the available vlan's and asks you to select the one you wish to delete. Click 'OK' to remove it.

Server Side Virtual LAN - xsadm console

Trustix Enterprise Firewall 4.1 has a modified Server Side GUI that allows users to enter the configuration information of the Virtual LANs. To configure the VLANs, the user can select 'Configure VLANs' option from the Main Menu. The user will be shown a new window where he will be prompted with options for adding, deleting, and modifying the VLANs. Depending on the user selection respective windows will opened to add, delete, or modify the VLAN's configuration. When the user saves the configuration of the VLAN, a script will run in the backend to bring up the new configuration.

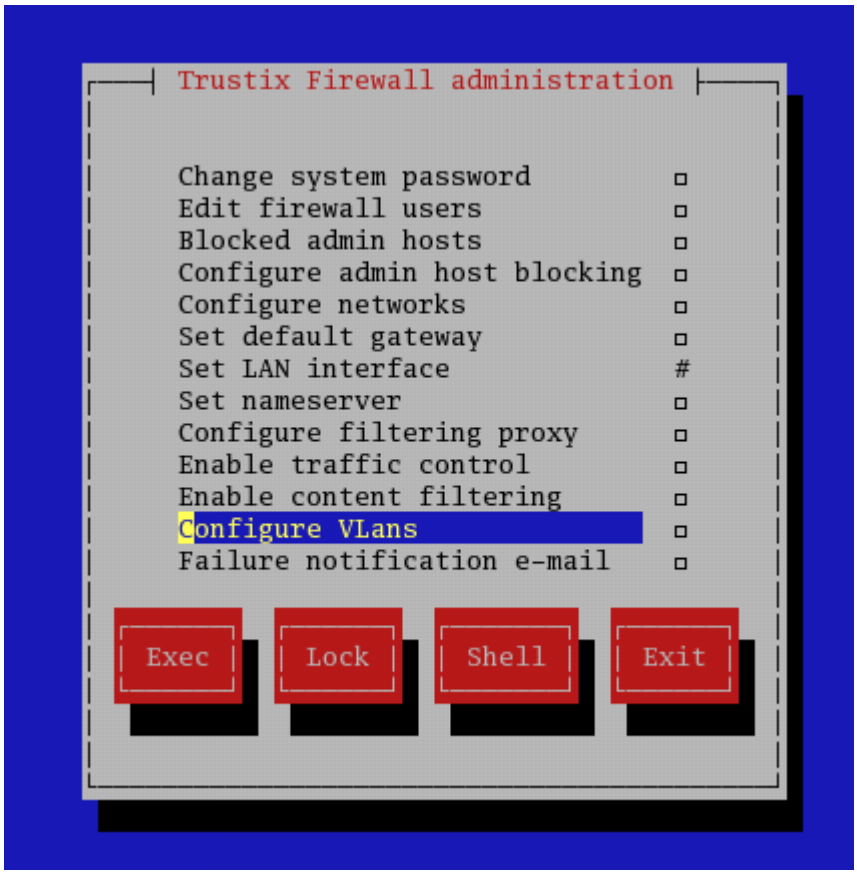


Figure G-5 Trustix Firewall Administration

Checking 'Configure VLANs' in the Firewall administration screen leads to the following configuration options:-

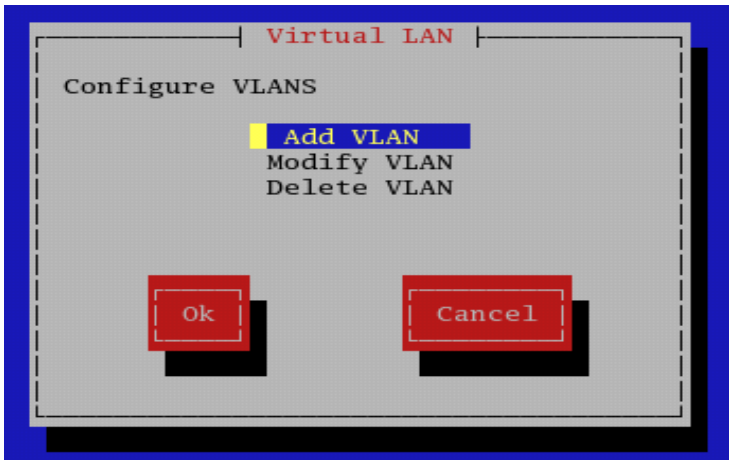


Figure G-6 Virtual LAN

Add VLAN

This option enables the administrator to configure settings concerning the new virtual lan. (see below)

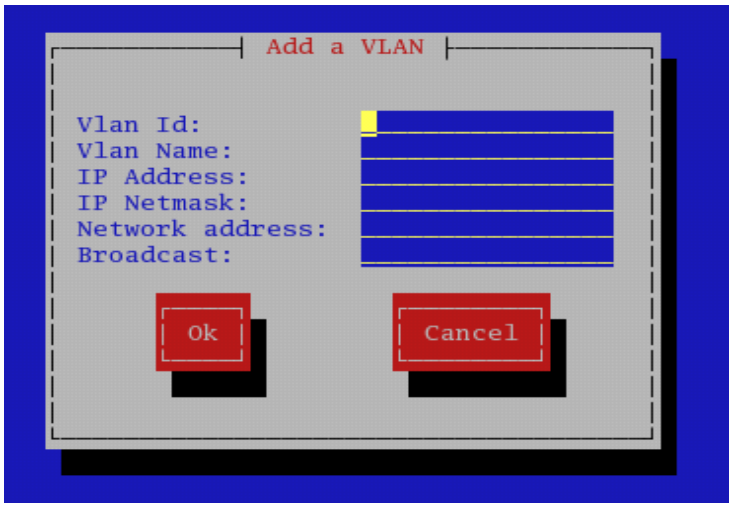


Figure G-7 Add a VLAN

Once you have entered the relevant information, click 'OK' to create the new VLAN.

Modify VLAN

As in the client side configuration, this option lists all the available VLANs that can be modified.

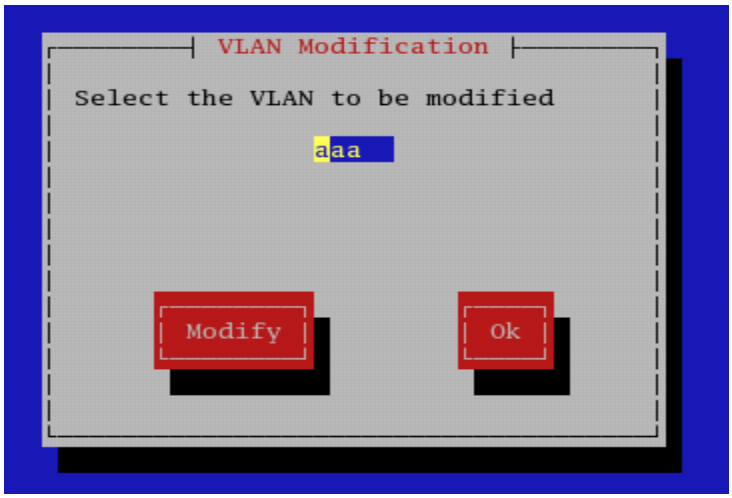


Figure G-8 VLAN Modification

Click a specific VLAN on the list and click 'OK'. You will then be presented with information pertaining to the particular VLAN and the ability to alter these settings as neccesary.

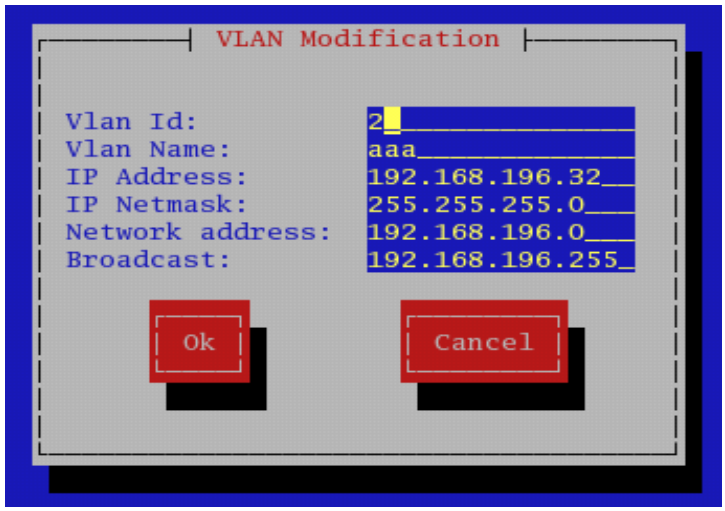


Figure G-9 VLAN Modification

Deleting VLAN

As in the 'add VLAN' section, the administrator will be presented with a list of all available vlan's . Select the one you wish to remove and select 'OK'

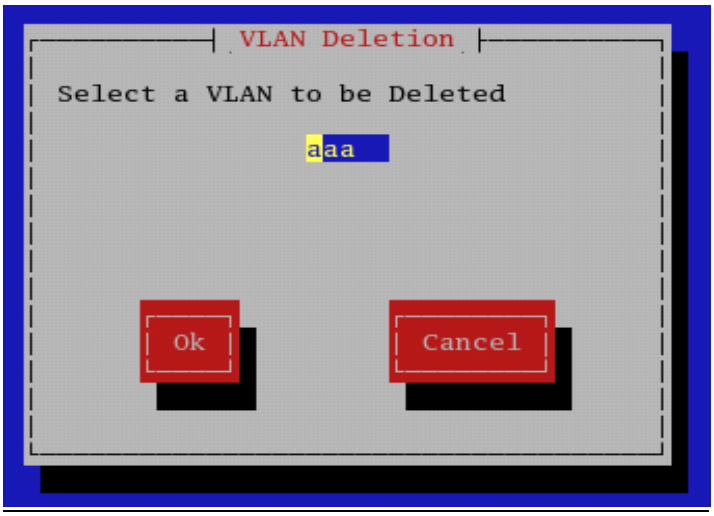


Figure G-10 VLAN Deletion

Trustix™

Appendix H

Traffic Shaping

Users can implement an effective traffic shaping setup that ensures that internet and network traffic can flow smoothly. By restricting certain types of traffic which may otherwise dominate the Internet link, Trustix Enterprise Firewall can optimize bandwidth and create a smoother and more efficient network.

Trustix Enterprise Firewall 4.1 allows the user to prioritize the network traffic which passes through the firewall. You can set priorities of your traffic to either high, medium or low as per your need. You can enable traffic control on any existing firewall accept rules.

Configuring traffic shaping policies in Trustix Enterprise Firewall is a two stage process. First you must enable it on the server side (xasdm console), then you set traffic priorities on the client side (xsentry client)

Server Side Traffic Shaping

Enabling/ Disabling Traffic Control

To enable traffic control, select the option “Enable traffic control” from the menu at the xasdm console. Click ‘Yes’ when the confirmation dialog appears. Enabling this setting allows users to manipulate traffic from the client. If traffic control is disabled at the server, it is not possible for clients to control traffic.

(See screenshots below)

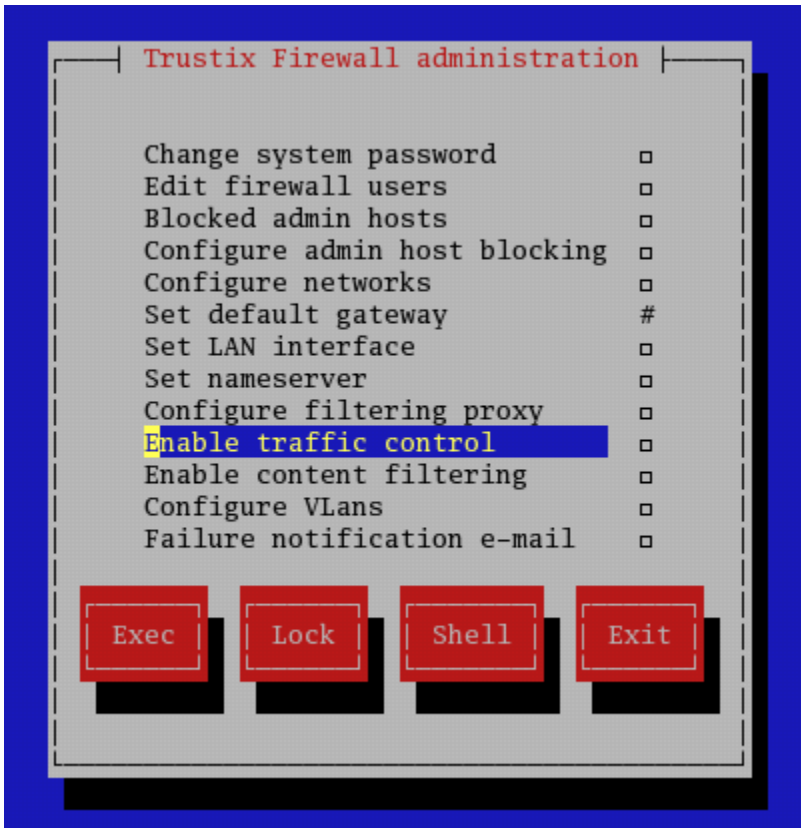


Figure H-1 Trustix Firewall administration

Selecting "Enable traffic control" leads to the following user confirmation dialog box.

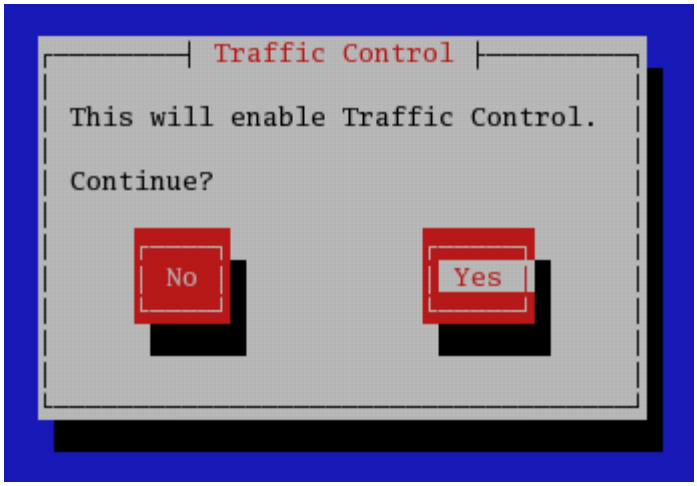


Figure H-2 Traffic Control

Selecting “Yes” will enable Traffic Control.

Similarly, if the user doesn't require this feature they can immediately disable it by selecting the option “Disable traffic control” at the server. This single click option removes all priority levels set by the client.

Client Side Traffic Shaping

Any rule in the GUI can be set with either low, medium or high priority by right clicking on the rule in the GUI and selecting the priority on the Priority Menu. When the configuration is being updated to the server, the set priority will be set to the corresponding rule.

There are four types of Traffic Shaping priorities can be set to any rule present in the Firewall client. Rules that have any priority set to them are represented on the XSentry GUI according to the priority they have been assigned:-

Low Priority. (rule is represented in **RED**)

Medium Priority. (rule is represented in **YELLOW**)

High Priority. (rule is represented in **GREEN**)

No Priority.

The default setting is ‘No priority’

Right click on a rule in the XSentry client. A menu will pop up as shown below.

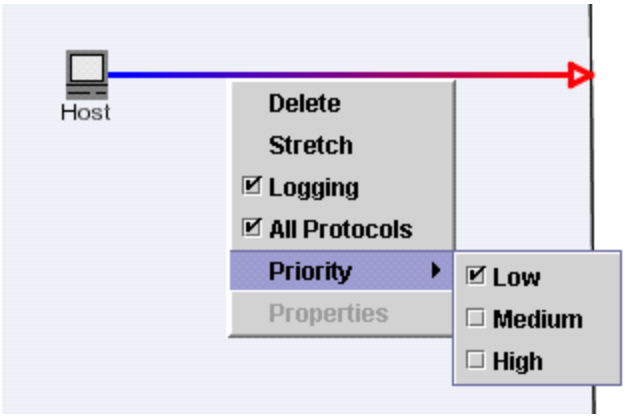


Figure H-3 Priority

Select ‘Priority’, then check the priority to be set to the selected rule. The example above shows a rule that has been assigned a ‘Low’ priority. (Note- Traffic Shaping must be enabled at the server for this prioritization to be possible)

If the user unchecks all priorities, the rule will revert to the default of ‘No Priority’

Traffic control tips

Protocols which transfer interactive traffic such as Telnet, SSH, FTP Control, TFTP, etc. will need more priority. This will improve the performance of the overall session. Whereas protocols such as FTP Data, SMTP, etc. which transfer bulk traffic should be set to medium priority. All other protocols ought to be set to low priority.

Trustix™

Appendix I

Microsoft Exchange Servers

Using Microsoft Windows Exchange servers behind a firewall can be a problem. This is because the Exchange server use dynamically bound ports for some services.

A solution to this problem involves binding these services (DS) to a specified (static binding) port and creating rules in your Trustix Firewall to allow traffic to these ports. The following ports are assigned on a Microsoft Exchange server:

Table I-1 MS Exchange server ports.

Service	Port
LDAP Authentication	389
LDAP with SSL	636
NNTP	119
POP3 Basic / NTLM	110
POP3 with SSL	995
IMAP4 Basic / NTLM	143
IMAP4 SSL	993
SMTP	25
Windows RPC End-point-mapper	135
MTA X.400	102
Named pipes	39

Allowing MAPI Client Access through a Firewall:

By default, the MS Exchange Server 5.5 will dynamically assign port numbers to be used for RPCs to access the directory or the Information store. Normally a MAPI client will connect to the server using port 135, which defines the Windows NT RPC-End-Point Mapper service. This service tells the client which dynamic port numbers it must use to access the directory and the Information Store. To assign fixed ports to these services you have to edit the registry. When it is configured, the firewall must be configured to allow TCP connections to the ports specified, and to port 135.

To set the static port numbers for the DS and IS, use regedit to add 2 new values to the registry. This is done on the Exchange Server.

For the Directory Service add an entry under the subkey:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDS\Parameters

The entry must be in the form of DWORD, called TCP/IP port and with the port number assigned as the value.

Example:

You want to assign port 1234 to the DS.

You will then have an entry under the subkey:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDS\Parameters,

called TCP/IP port with a value of 1234.

For the Information Store add an entry under the subkey:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem

Again, the entry must be in the form of DWORD, called TCP/IP port and with the port number assigned as the value.

Trustix™

Appendix J

Licences

Trustix Secure Linux Products

Trustix™ Enterprise Firewall, CLIENT SOFTWARE

Trustix™ Enterprise Firewall, SERVER SOFTWARE

Trustix™ Enterprise Firewall, SERVER LICENSE KEY.

Trustix™ Enterprise Firewall, SERVER LICENSE CERTIFICATE

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), WHICH SETS FORTH SUBSCRIPTION TERMS FOR TRUSTIX PRODUCTS IDENTIFIED IN THE HEADING ABOVE ("SOFTWARE"). BY INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT WITH TRUSTIX INC. IF YOU DO NOT AGREE TO ALL OF ITS TERMS, DO NOT INSTALL THE SOFTWARE, OR DESTROY ALL COPIES OF THE SOFTWARE THAT YOU HAVE INSTALLED. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

1. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, TRUSTIX INC. hereby grants to you a non-exclusive, non-transferable right to use the amount of "server license keys" (see under) in the use of the specified version of the Software, and the accompanying documentation (the "Documentation").

You may install one copy of the Server Software on one server (computer) for which the Software was designed. The Client Software may be installed on workstations (computers), for which the software was designed. If the Software is licensed as a suite or bundle with more than one specified Software products, this license applies to all such specified Software product, subject to any restrictions or usage terms specified individually for any of such Software products on the applicable product invoicing or packaging.

Server license keys/certificates. Either a "server license key" or a "server licence certificate" is required to activate the Trustix Inc. Enterprise Firewall Software. The software is TRUSTIX INC. property. The customer has the right to use it according to this Agreement only.

2. Software and all associated intellectual property rights are retained by TRUSTIX INC. and/or its licensors. Except as specifically authorized in any Supplemental License Terms, you may not make copies of Software, other than a single copy of Software for archival purposes. Unless enforcement is prohibited by applicable law, you may not modify, decompile, reverse engineer Software. You may not publish or provide the results of any benchmark or comparison tests run on Software to any third party without the prior written consent of TRUSTIX INC. No right, title or interest in or to any trademark, service mark, logo or trade name of TRUSTIX INC. or its licensors is granted under this Agreement. You may not rent, lease, loan or resell the Software. You may not transfer any of the rights you have subscribed under this Agreement. You may not modify, or create derivative works based upon, the Software in whole or in part, except as specifically authorized in any Supplemental License Terms. You may not copy the Software or Documentation except as expressly permitted in written by TRUSTIX INC. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by TRUSTIX INC. TRUSTIX INC. reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

3. Server Use. A separate server license key or server licence certificate, downloaded from http://www.trustix.com or an authorized dealer, is required for each server that may connect to the Client Software at any time, regardless of whether such servers are connected to the Software concurrently, or are actually using the Software at any particular time. If the number of servers that can connect to the Software can exceed the number of server license keys, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the server license keys. This Agreement authorizes you to make or download one copy of the Documentation for each server license, provided that each such copy contains all of the proprietary notices for the Documentation.

4. Term. This Agreement is effective until you or TRUSTIX INC. terminates the Agreement earlier, in accordance with the terms set forth herein. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. This also if the customers or users use of the Software or services makes significant problems for other users or TRUSTIX INC. Termination of the Agreement also if, according to TRUSTIX INC.' entitled estimate, customer or user abuse the Software or one of these tries to abuse it. When this Agreement terminates, TRUSTIX INC. will stop the services and use of the Software immediately. When this Agreement terminates, you must destroy all copies of the Software and the Documentation.

5. Updates. You may download revisions, upgrades, or updates to this version of the Software if and as TRUSTIX INC. publishes them via its web site http://www.trustix.com

6. Ownership Rights. The Software is protected by Norwegian copyright laws and international treaty provisions. TRUSTIX INC. own the Software, TRUSTIX INC. and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. You acknowledge that your server license keys and use of the Software does not transfer to you any title to the intellectual property in the Software, and that you will not acquire any rights to the Software except as expressly set forth in this Agreement. You agree that any copies of the Software and Documentation will contain the same proprietary notices that appear on and in the Software and Documentation.

7. Warranty and Disclaimer

a. Limited Warranty. TRUSTIX INC. warrants that for one year from the date of original purchase, the media (for example, the CD-rom) on which the Software is contained will be free from defects in materials and workmanship.

b. Customer Remedies. TRUSTIX INC.'s and its suppliers' entire liability, and your exclusive remedy, shall be, at TRUSTIX INC.'s option, either (i) to return the purchase price paid for the license, if any, or (ii) to replace the defective media on which the Software is contained with a copy on nondefective media. You must return the defective media to TRUSTIX INC. at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period.

c. Warranty Disclaimer. To the maximum extent permitted by applicable law, and except for the limited warranty set forth therein, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING PROVISIONS, YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, TRUSTIX INC. MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES, OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TRUSTIX INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THE FOREGOING PROVISIONS SHALL BE ENFORCEABLE TO THE MAXIMUM EXTENT PERMITTED BY THE APPLICABLE LAW.

8. Limitation of Liability. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL TRUSTIX INC. OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL TRUSTIX INC. BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE SUBSCRIPTION PRICE TRUSTIX INC. CHARGES FOR A SUBSCRIPTION TO THE SOFTWARE, EVEN IF TRUSTIX INC. SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MIGHT NOT APPLY TO YOU. THE FOREGOING PROVISIONS SHALL BE ENFORCEABLE TO THE MAXIMUM EXTENT PERMITTED BY THE APPLICABLE LAW.

9. Export Regulations. All Software and technical data delivered under this Agreement are subject to UK export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you. TRUSTIX INC. HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

10. High Risk Activities. The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). TRUSTIX INC. EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR High Risk Activities.

11. JURISDICTION. THIS AGREEMENT IS GOVERNED BY THE LAWS OF ENGLAND, WITHOUT REFERENCE TO CONFLICT OF LAWS PRINCIPLES. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded.

12. Miscellaneous. This Subscription Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. This Subscription Agreement supersedes any other communications with respect to the Software and Documentation. This Subscription Agreement may not be modified except by a written addendum issued by a duly authorized representative of TRUSTIX INC. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by TRUSTIX INC. or a duly authorized representative of TRUSTIX INC. If any provision of this Subscription Agreement is held invalid, the remainder of this Subscription Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Subscription Agreement has been written in the English language only.

13. TRUSTIX INC. CUSTOMER CONTACT. If you have any questions concerning these terms and conditions, or if you would like to contact TRUSTIX INC. for any other reason, please call:

(+44) 161 8747080, fax (+44) 161 8771767

TRUSTIX INC

or visit the web site at http://www.trustix.com

e-mail : trustix@trustix.com

Trustix™

Appendix K

Trustix Technical Support

Trustix is committed to providing comprehensive technical support. Before contacting our technical support department, please try to resolve all possible problems by using this guide, the on-line help system and the Trustix™ website available at

`http://www.trustix.com`

Technical support for products from Trustix is available to registered customers. Support packages will have been agreed when the firewall was licensed. Priority support is given to customers that have either purchased a Service and Upgrade Agreement or purchased a Support Agreement. Support is available by phone, fax and online. Registration can be done by contacting sales@trustix.com

Registered customers are entitled to use the XSentry support website, which includes updated information, firewall solutions and knowledge base. In order to receive support, please have your order number available. This can be found on the email that you received with the license attached.

Premium Technical Phone Support

You are able to talk to our dedicated team of experts by dialing the Premium Technical Support Phone number shown below. (Calls will be charged directly to your phone account, and please note that call charges from some mobiles and fixed lines may vary depending on the telephone operator). Please have the product details, account number any other necessary information that will allow us to deal with your query as efficiently as possible.

0906 436 8070 Premium Technical Support Phone

Hours of operation:

9:00AM to 10:00PM CET Monday through Friday (excluding major holidays)

Cost is 50p per minute, billed to your phone bill

This support line is available to users of all Trustix™ products not just the Enterprise Firewall.

Trustix™

Appendix L

DHCP Server and Relay Support

DHCP Server

The DHCP Module consists of DHCP Server and DHCP Relay.

To configure DHCP Server on your system, you need to provide the following three types of information:

- DHCP Common
- IP Pools
- Static Host

To navigate to **DHCP Server Configuration** section,

- Click **Server** -> **DHCP**

The **DHCP Server Properties** screen appears

DHCP Common

To navigate to **DHCP Common** section,

- Click **DHCP Common** tab

To configure DHCP Server properties, follow the steps given below:

- Enter the Primary DNS IP address in **Primary DNS** field
- Enter the maximum lease time in **Max Lease Time** field
- Enter the default lease time in the **Default Lease Time** field
- Click **Save**

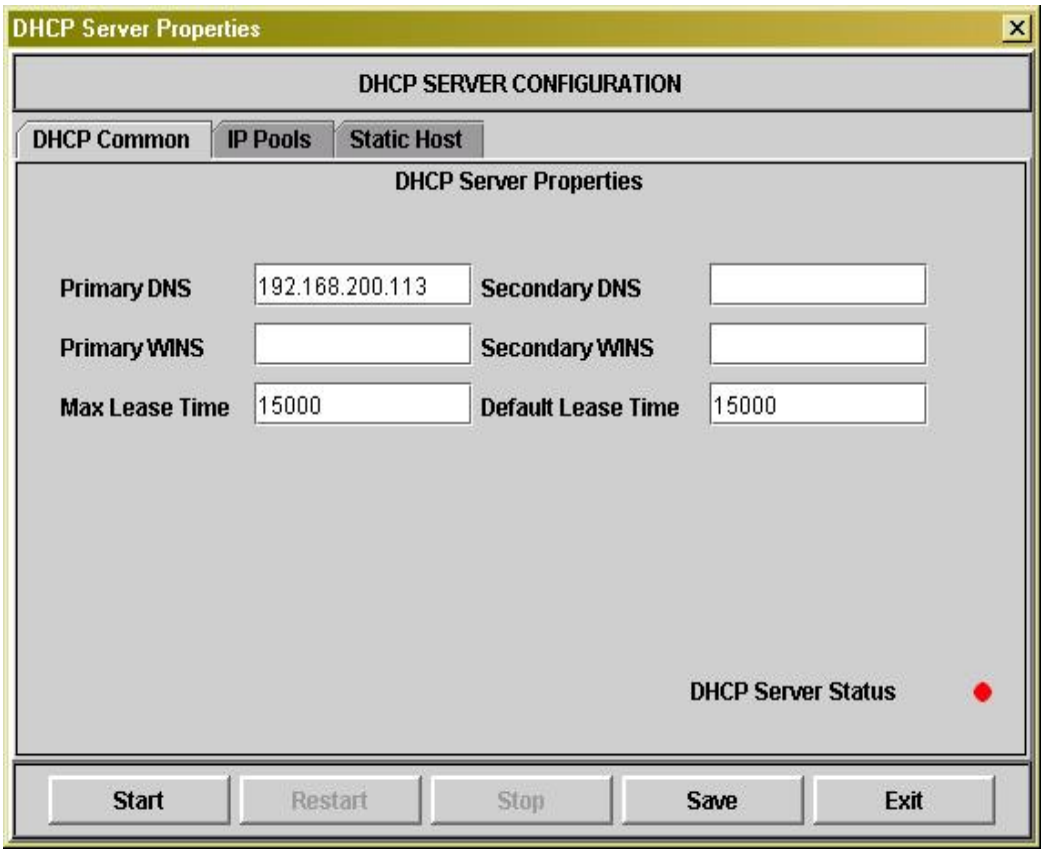


Figure L-1 DHCP Common

IP Pools

To assign the range of IP Address in the subnet for generating IP Address automatically, you have to create IP Pools. All the existing IP pools will be displayed initially.

To navigate to **IP Pools** section,

- Click on **IP Pools** tab

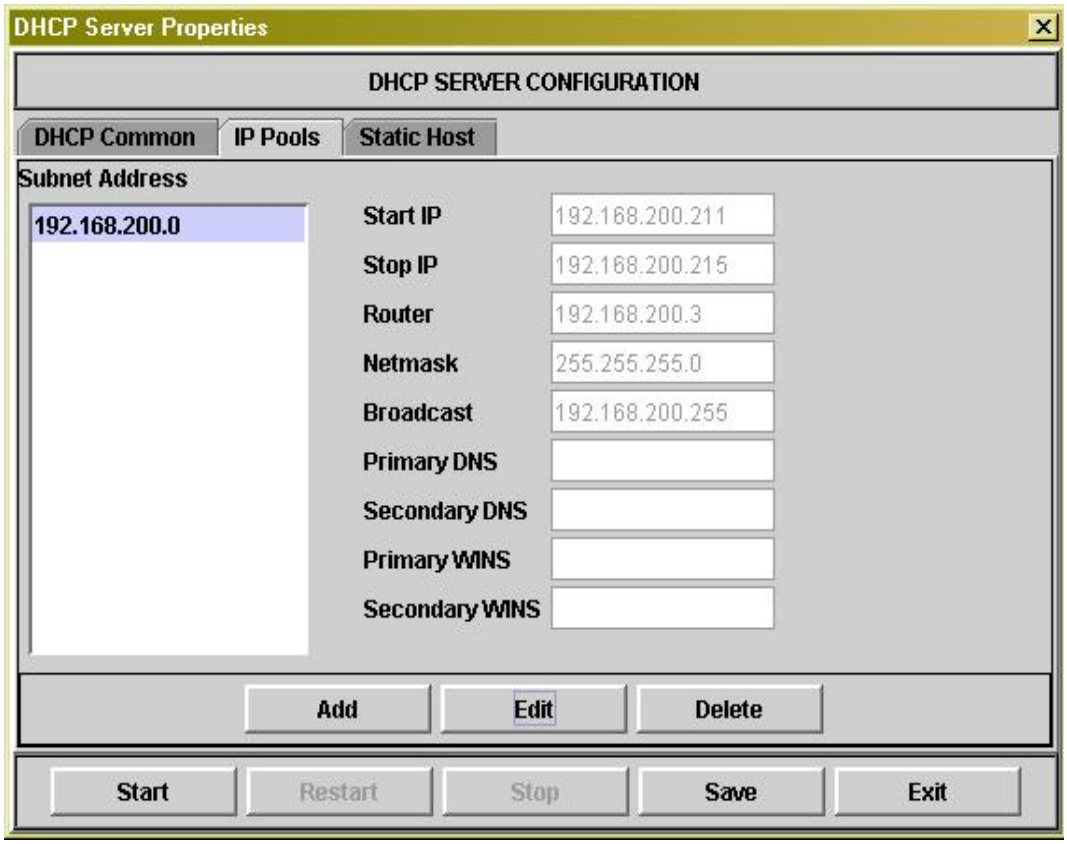


Figure L-2 IP Pools

To create a new IP Pool, click on the **Add** button.

To edit an existing IP Pool, follow the steps given below:

- Select the required subnet address from **Subnet Address** field.
- Click **Edit**

To delete an IP Pool, click **Delete**

Static Host

To configure Static host, enter the required Static host information.

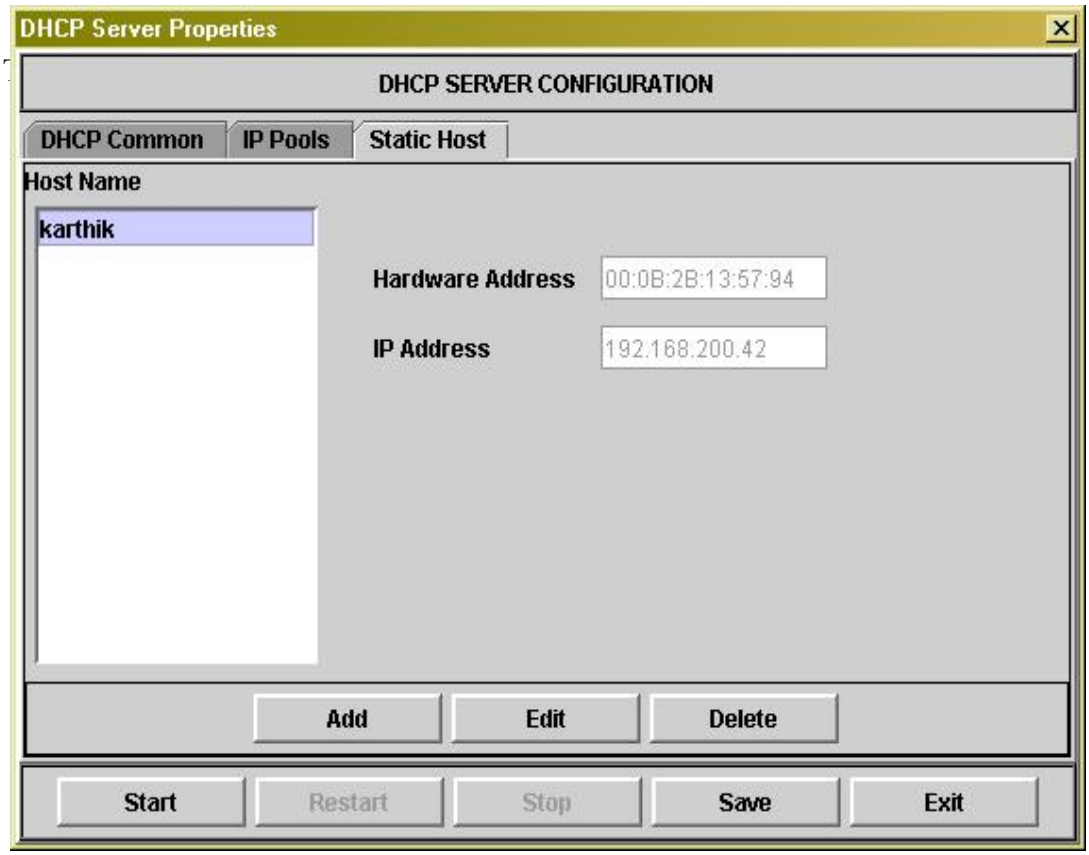


Figure L-3 Static Host

To add a Static host, click **Add**

Note: You can add more than one Static host to a DHCP Server.

To edit a Static host, follow the steps given below:

- Select the required Static host from the **Host Name** field.
- Click **Edit**

To delete a Static host, click **Delete**

After providing the entire information, to save all the configuration information on the DHCP Server, click **Save**

To start the DHCP Server, click **Start**. To stop the DHCP Server, click **Stop**. To restart the DHCP Server, click **Restart**

DHCP Relay

To configure DHCP Relay, you must provide the DHCP Server and broadcast information.

To navigate to **DHCP Relay** screen,

- Click **Server** -> **DHCP**

After providing the entire information, to save all the configuration information on the DHCP Server, click **Save**.

To start the DHCP Relay, click **Start**. To stop the DHCP Relay, click **Stop**. To restart the DHCP Relay, click **Restart**.

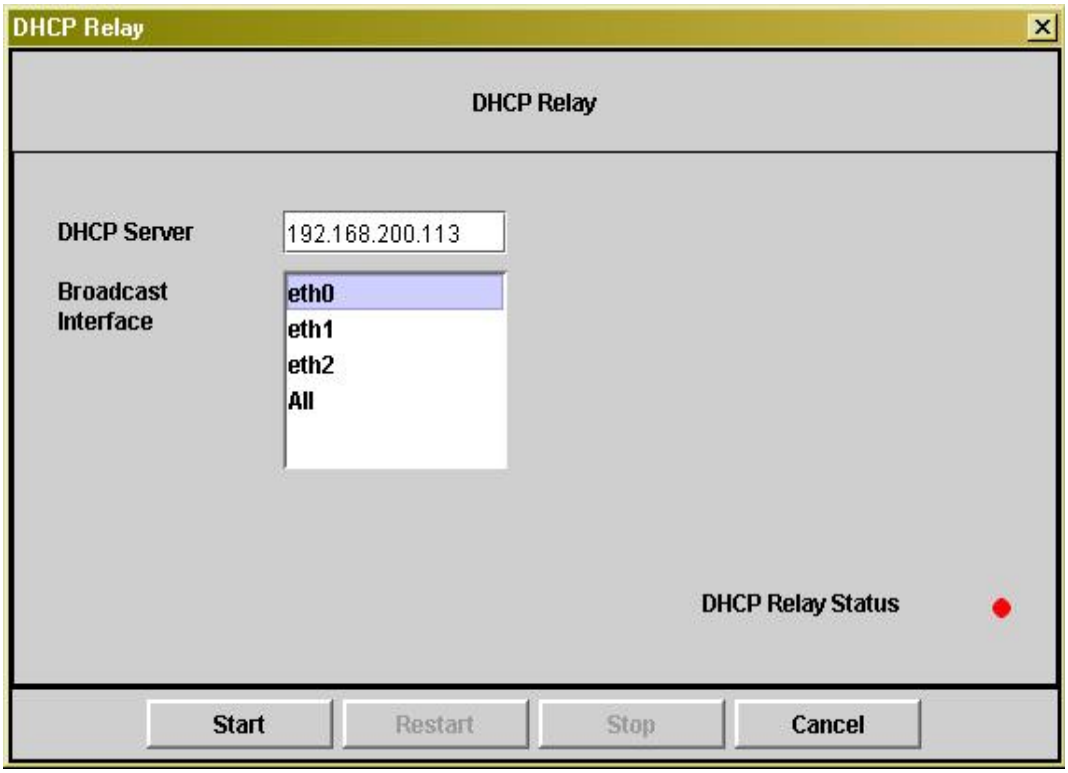


Figure L-4 DHCP Relay

Trustix™

Appendix M

Monitoring and Alerts

Monitoring

To navigate to the **Monitor Menu** screen,

- Click **Firewall** -> **Monitoring**

The following **Monitor Menu** screen appears

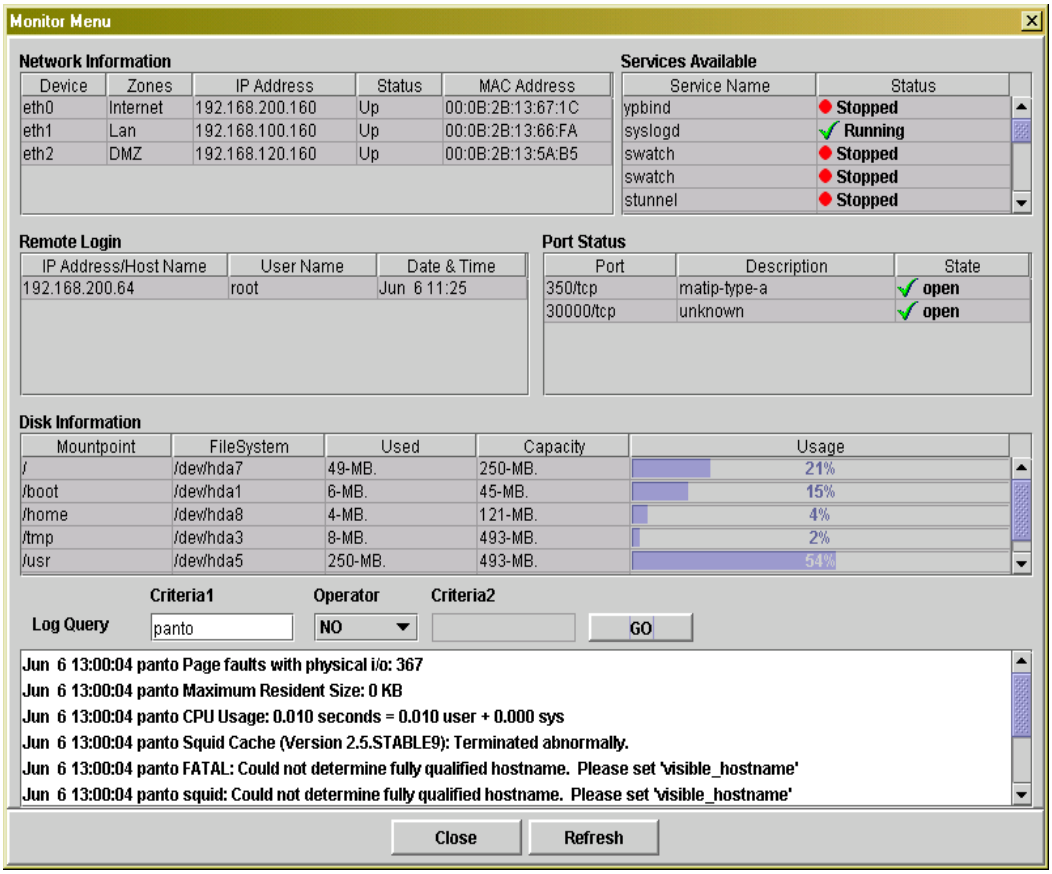

Monitor Menu
Network Information
Device Zones IP Address Status MAC Address
eth0 Internet 192.168.200.160 Up 00:0B:2B:13:67:1C
eth1 Lan 192.168.100.160 Up 00:0B:2B:13:66:FA
eth2 DMZ 192.168.120.160 Up 00:0B:2B:13:5A:B5
Services Available
Service Name Status
ypbind Stopped
syslogd Running
swatch Stopped
swatch Stopped
stunnel Stopped
Remote Login
IP Address/Host Name User Name Date & Time
192.168.200.64 root Jun 6 11:25
Port Status
Port Description State
350/tcp matip-type-a open
30000/tcp unknown open
Disk Information
Mountpoint FileSystem Used Capacity Usage
/ /dev/hda7 49-MB. 250-MB. 21%
/boot /dev/hda1 6-MB. 45-MB. 15%
/home /dev/hda8 4-MB. 121-MB. 4%
/tmp /dev/hda3 8-MB. 493-MB. 2%
/usr /dev/hda5 250-MB. 493-MB. 54%
Criteria1 Operator Criteria2
Log Query panto NO GO
Jun 6 13:00:04 panto Page faults with physical i/o: 367
Jun 6 13:00:04 panto Maximum Resident Size: 0 KB
Jun 6 13:00:04 panto CPU Usage: 0.010 seconds = 0.010 user + 0.000 sys
Jun 6 13:00:04 panto Squid Cache (Version 2.5.STABLE9): Terminated abnormally.
Jun 6 13:00:04 panto FATAL: Could not determine fully qualified hostname. Please set 'visible_hostname'
Jun 6 13:00:04 panto squid: Could not determine fully qualified hostname. Please set 'visible_hostname'
Close
Refresh

Figure M-1 Monitor Menu

The **Monitor Menu** screen provides the following information.

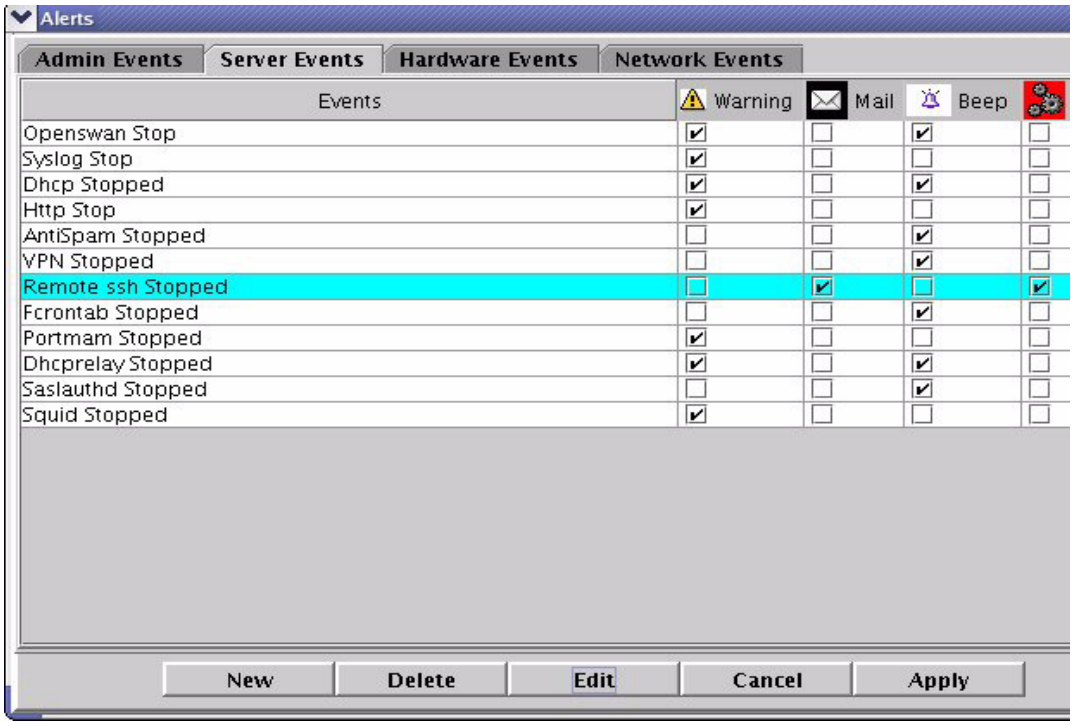
- **Network Information –** Displays the details of each device (IP address, Status, Zone name and the MAC address) available in the firewall
- **Services Available –** Displays the details of all the services (name and status) available in the firewall
- **Remote Login –** Displays the details of all the remote machines (IP address, user name and date & time) logged into the firewall
- **Port Status –** Displays the details of all the ports (description and state) available in the firewall
- **Disk Information -** Displays the details of all the disks (Mountpoint, filesystem, capacity, usage) available in the firewall
- **Log Query –** Displays important log information of the firewall depending upon the specified search string

Alerts

To navigate to the **Alerts** screen,

- Click **Firewall** -> **Alerts**

The following **Alerts** screen appears



Example M-1 Alerts

Adding Alerts

To add **Alerts,**

- Click **New** button in the **Alerts** screen

The following **Alerts** screen appears

Figure M-2 Add Alerts

- Enter all the necessary information and click **OK** button
- Click **Apply** button to save all the changes made

Note: Any number of alerts can be added in any category.

Deleting Alerts

To delete **Alerts,**

- Select an alert to be deleted in the **Alerts** screen and click **Delete** button
- Click **Apply** button to save all the changes made

Editing Alerts

To edit **Alerts,**

- Select an alert to be edited in the **Alerts** screen and click **Edit** button

The following **Alerts** screen appears

Figure M-3 Modify Alerts

- Make the necessary information and click **OK** button
- Click **Apply** button to save all the changes made

The following **Alerts Saved** message box displaying the message, **Alerts configuration updated successfully** appears

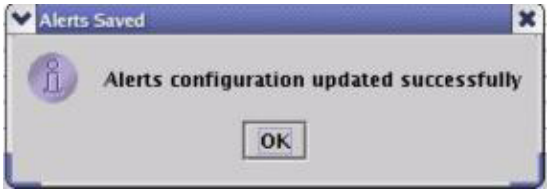


Figure M-4 Alert Updation Confirmation

Trustix™

Appendix N

Network Configuration

To navigate to **Network Configuration** option,

- Select **Administration** -> **Network Configuration**

The **Network Configuration** dialog box appears

Devices Configuration

To navigate to **Devices** section,

- Click on **Devices** tab

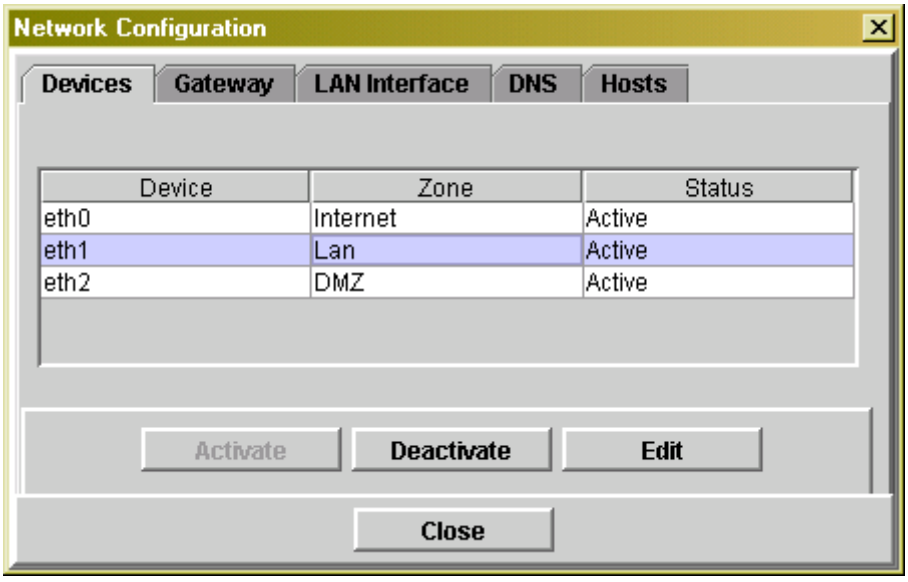


Figure N-1 Device Configuration

To activate a device, follow the steps given below:

- Select the required device
- Click **Activate**

Note: If the device is already activated then the **Activate** button will be disabled while selecting this device.

To deactivate a device, follow the steps given below:

- Select the required device
- Click **Deactivate**

Note: If the device is already deactivated then the **Deactivate** button will be disabled while selecting this device.

To edit the device information, follow the steps given below:

- Select the required device
- Click **Edit**

The **Edit Network Interface Card** screen appears

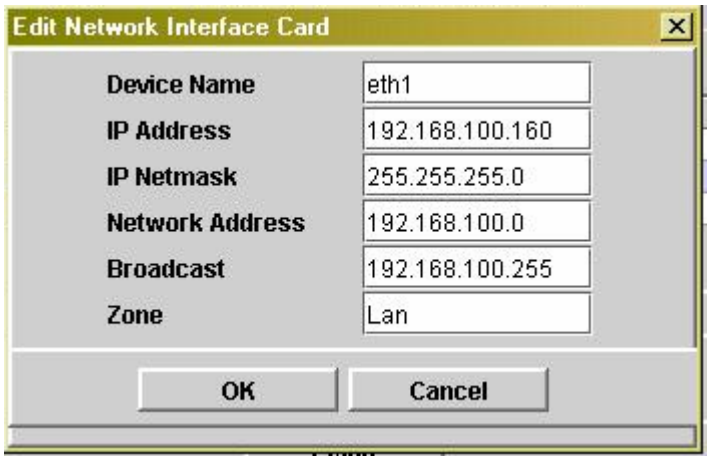


Figure N-2 Edit Network Interface Card

- Make the necessary modifications
- Click **OK** to save changes

Gateway Configuration

To navigate to **Gateway** section,

- Click on **Gateway** tab

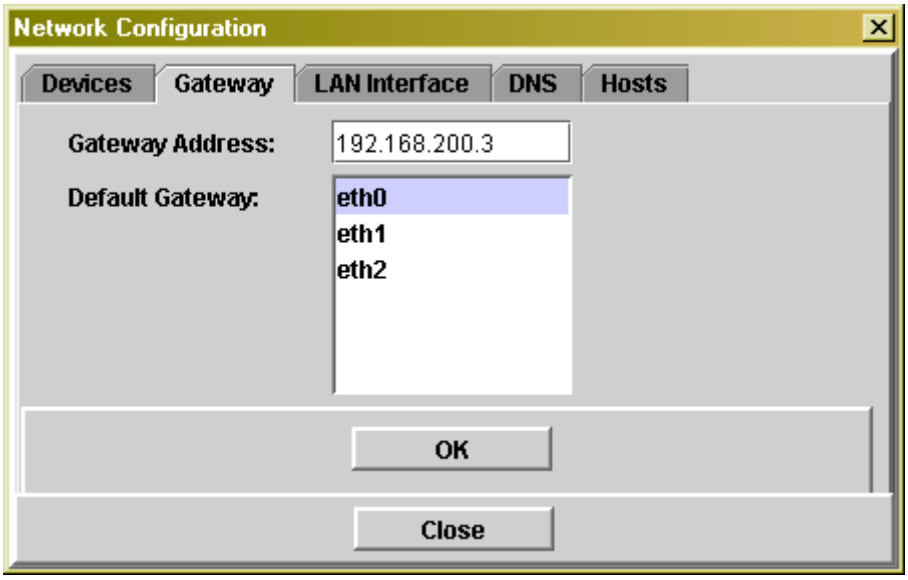


Figure N-3 Gateway Configuration

This section displays the gateway address and various gateway devices of the Firewall server that are already configured.

To change the gateway address or the gateway device, follow the steps given below:

- Make the necessary changes
- Click **OK**
- Click **Close** to close **Network Configuration** screen

LAN Configuration

To navigate to **LAN Interface** section,

- Click on **LAN Interface** tab

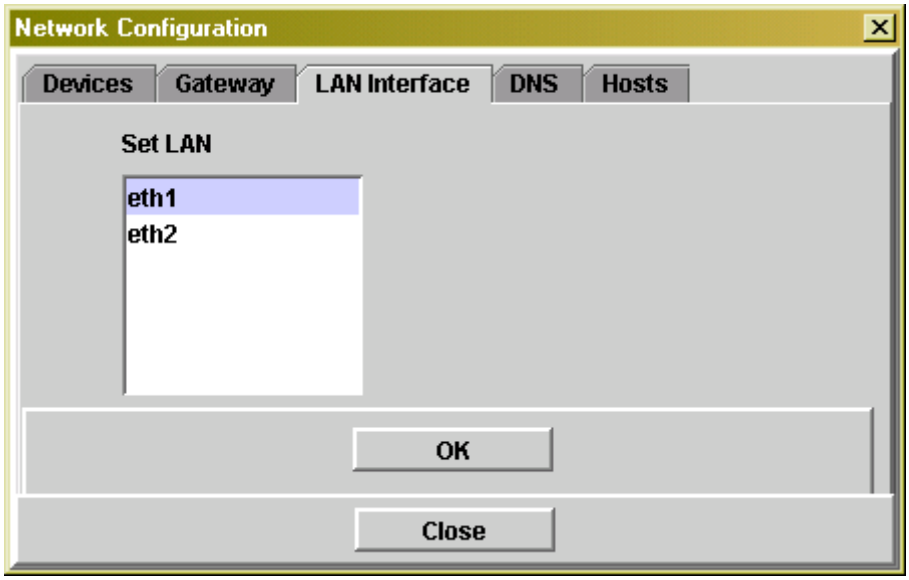


Figure N-4 LAN Interface Configuration

This section displays the LAN device of the Firewall Server that is already configured.

To change the LAN device, follow the steps given below:

- Make the necessary changes
- Click **OK**
- Click **Close** to close **Network Configuration** screen

DNS Configuration

To navigate to **DNS** section,

- Click on **DNS** tab

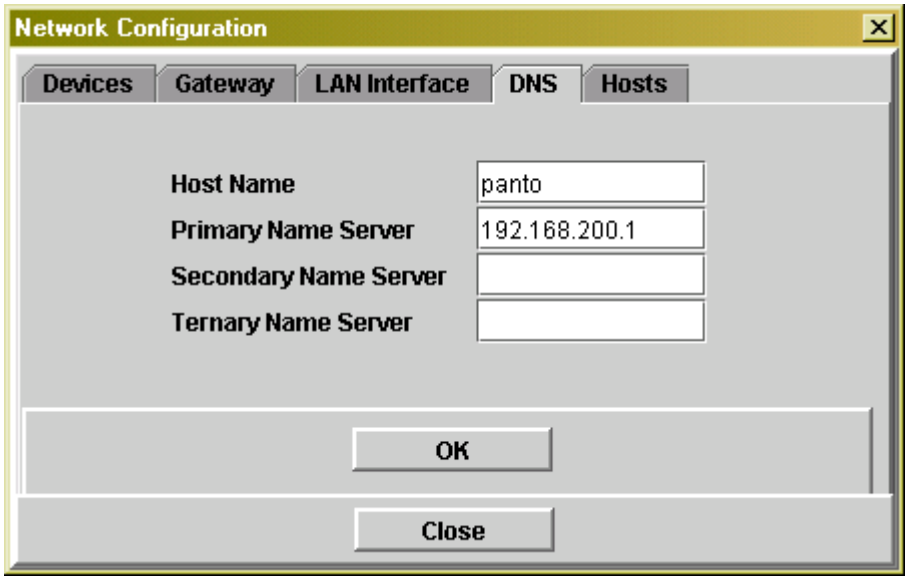


Figure N-5 DNS Configuration

This section displays the Hostname, Primary name server, Secondary name server and Ternary name server.

The **Host Name** field is mandatory. In other words, you cannot leave it blank. The **Primary Name Server**, **Secondary Name Server** and the **Ternary Name Server** fields are not mandatory.

Note: After making necessary modifications, you have to restart the Firewall Server to implement the change.

Hosts Configuration

To navigate to **Hosts** section,

- Click on **Hosts** tab

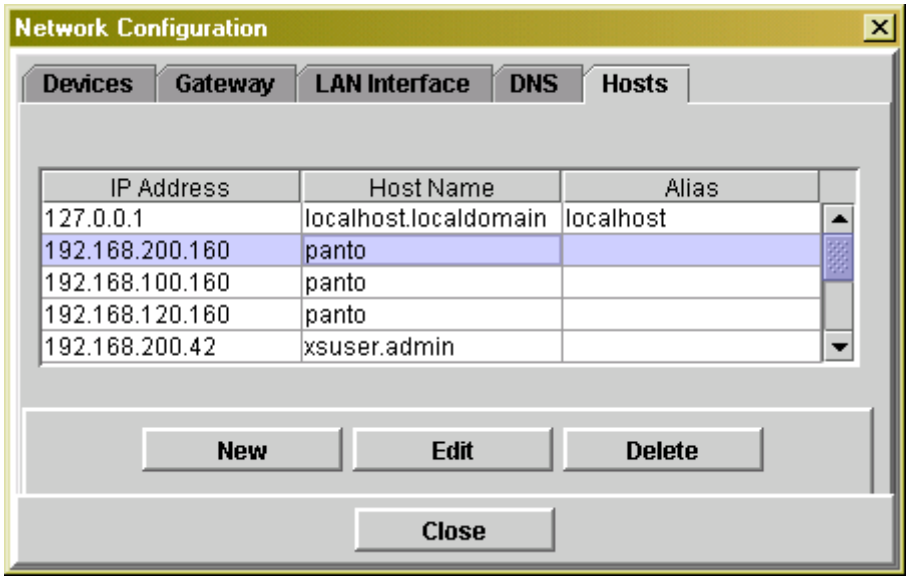


Figure N-6 Hosts Configuration

Adding Host

To create a new host, follow the steps given below:

- Click **New**

The **Add New Host** screen appears

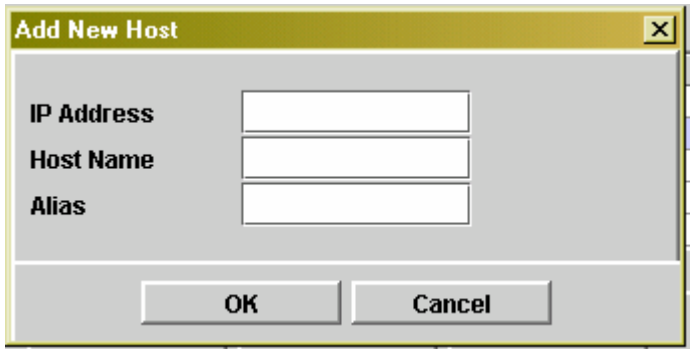


Figure N-7 Add New Host

- Enter the necessary information
- Click **OK**

Note: The **IP Address** and **Host Name** fields are mandatory.

Edit Host

To edit Host information, follow the steps given below:

- Select the host to be modified
- Click **Edit**

The **Edit Host** screen appears

- Make the necessary modifications

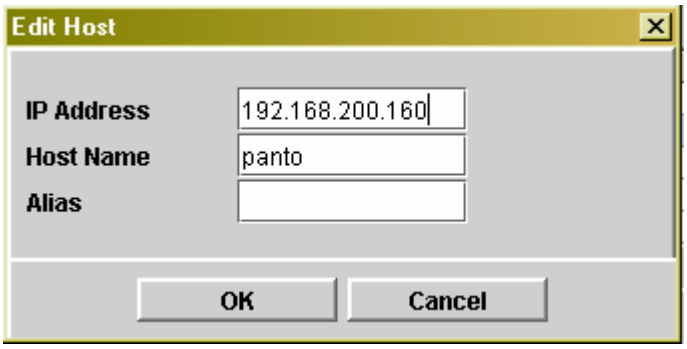


Figure N-8 Edit Host

- Click **OK**

Note: The **IP Address** and **Host Name** fields are mandatory.

Delete Host

To delete a host, follow the steps given below:

- Select the host that is to be deleted
- Click **Delete**

Trustix™

Appendix O

ARP Proxy

To navigate to Proxy ARP option,

- Click **Firewall** -> **ARP Proxy**

The **Proxy ARP** screen appears. It displays all the existing ARP Proxies in the Firewall

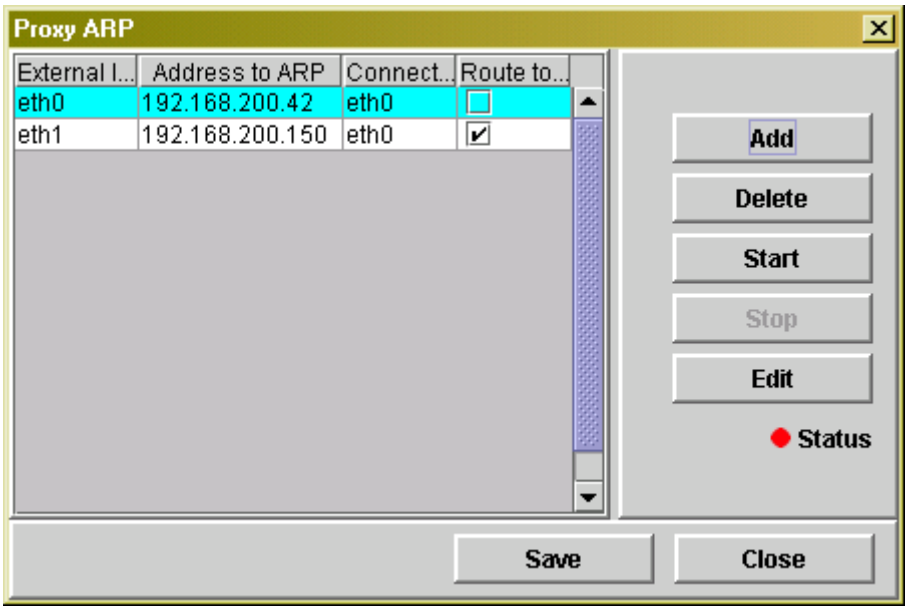


Figure O-1 Proxy ARP

Add ARP Proxy

To add an ARP Proxy, follow the steps given below:

- Click **Add**

The **Add Proxy** screen appears

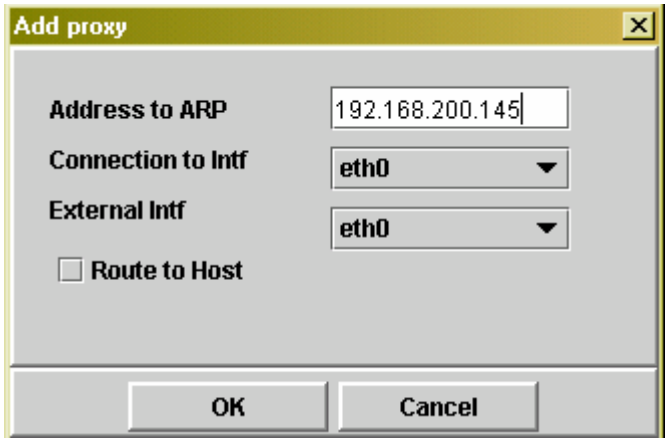


Figure O-2 Add Proxy

- Enter the necessary information
- Click **OK**

Edit ARP Proxy

To edit an ARP Proxy, follow the steps given below:

- Select the ARP Proxy to be modified
- Click **Edit**
- Make the necessary changes
- Click **OK**

Delete ARP Proxy

To delete an ARP Proxy, follow the steps given below:

- Select the ARP Proxy to be deleted
- Click **Delete**

To start the ARP Proxy Server, click **Start**. To stop the ARP Proxy Server, click **Stop**.

Trustix™

Appendix P

Advanced Logging

Display Configuration

To navigate to the **Display Configurations** screen,

- Click **Firewall logs** -> **DisplayConfigurations**

The following **Firewall Log Configuration** screen appears

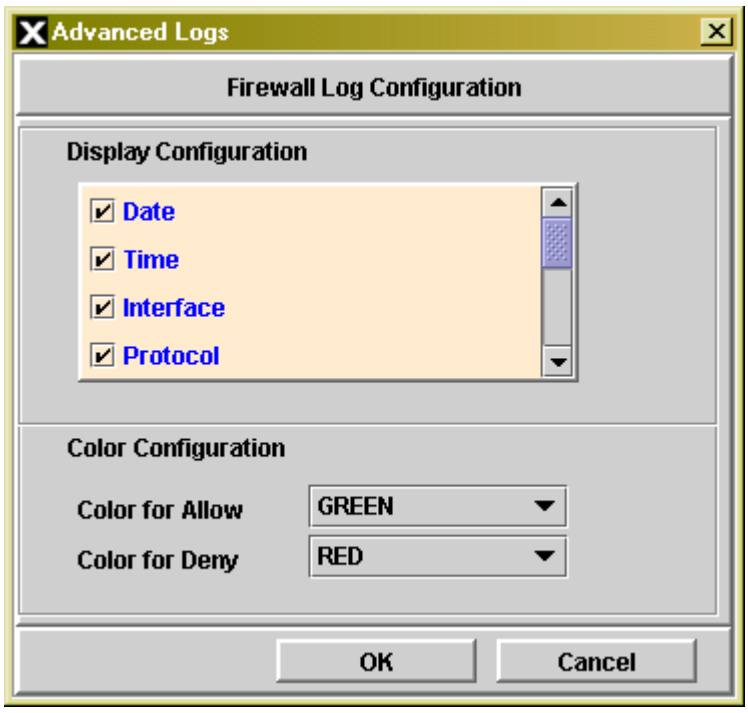


Figure P-1 Firewall Log Configuration

The **Firewall Log Configuration** screen displays the header information for the Firewall Log Search.

To configure Firewall Logs, follow the steps given below:

- Select the header information to be displayed in the result table from the **Display Configuration** section
- Choose a color for the firewall log search result indicating the **Allow** rule from the **Color Configuration** section
- Choose a color for the firewall log search result indicating the **Deny** rule from the **Color Configuration** section
- Then, click **OK** button

LogRotate Configuration

To navigate to the **Log Rotate Configurations** screen,

- Click **Firewall logs** -> **Log Rotate Configuration**

The following **Log Rotate Configuration** screen appears

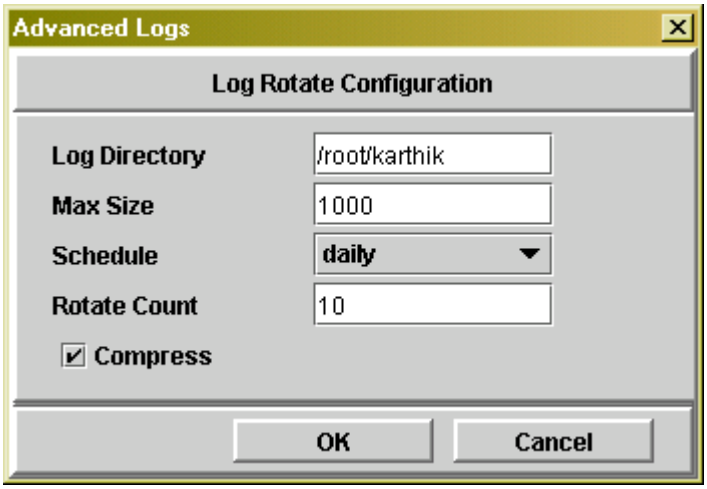


Figure P-2 Log Rotate Configuration

To configure rotated Logs, follow the steps given below:

- Enter the directory where the rotated log files have to be placed in the **Log Directory** field
- Enter the size limit after which the log file have to be rotated in the **Max Size** field
- Choose either of the options listed in the following table from the **Schedule** dropdown list

Option	Description
Daily	The log file will be rotated daily
Weekly	The log file will be rotated weekly
Monthly	The log file will be rotated monthly

- Enter the maximum number of rotated log file to be present in the log directory at any moment in the **Rotate Count** field
- Select the **Compress** check box to compress and rotate the log file
- Then, click **OK** button

Firewall Log Search

To navigate to the **Firewall Log Search** screen,

- Click **Firewall logs** -> **Firewall Log Search**

The following **Firewall Log Search** screen appears

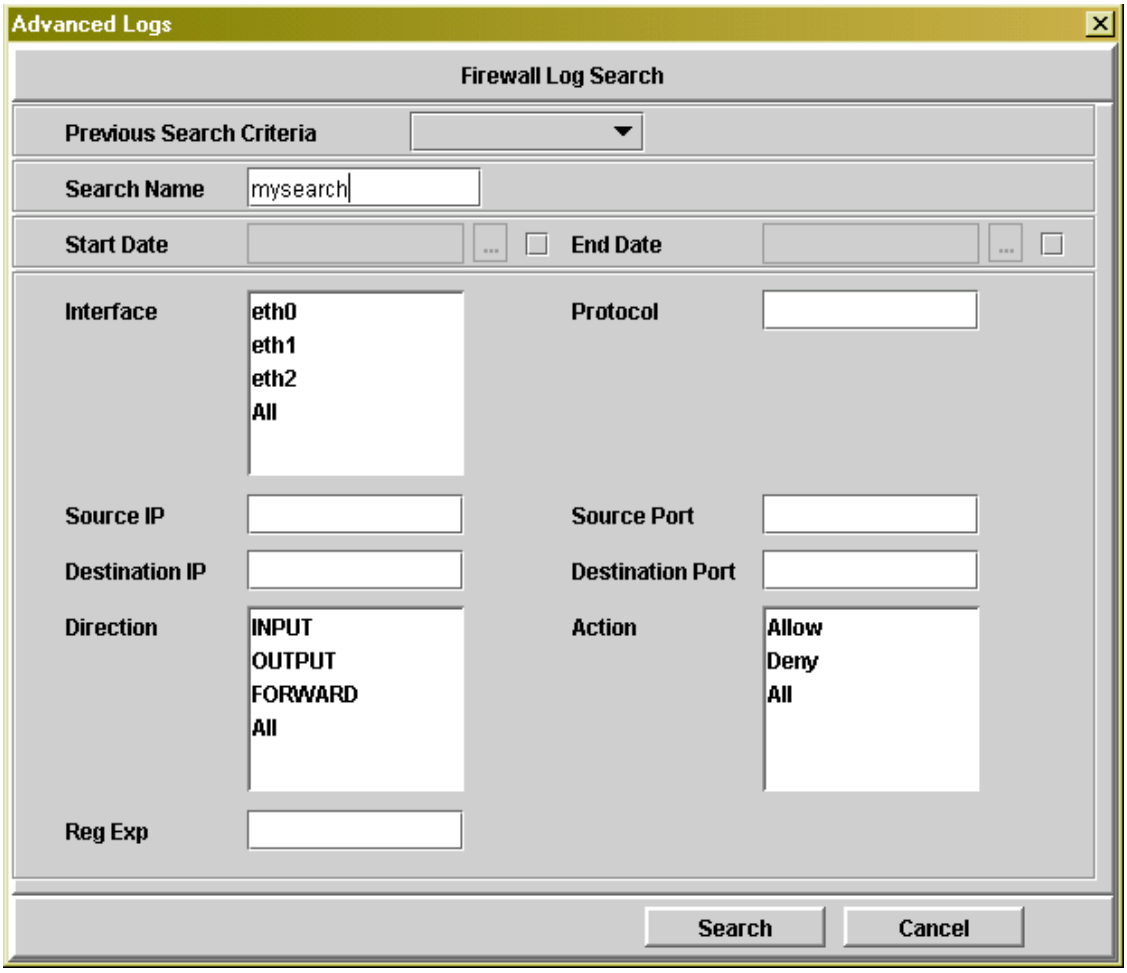


Figure P-3 Firewall Log Search

To perform a **Firewall Log Search,**

- Enter all the search criteria information in the fields provided in the **Firewall Log Search** screen
- Click **Search** button

The following **Log Search Result** screen appears

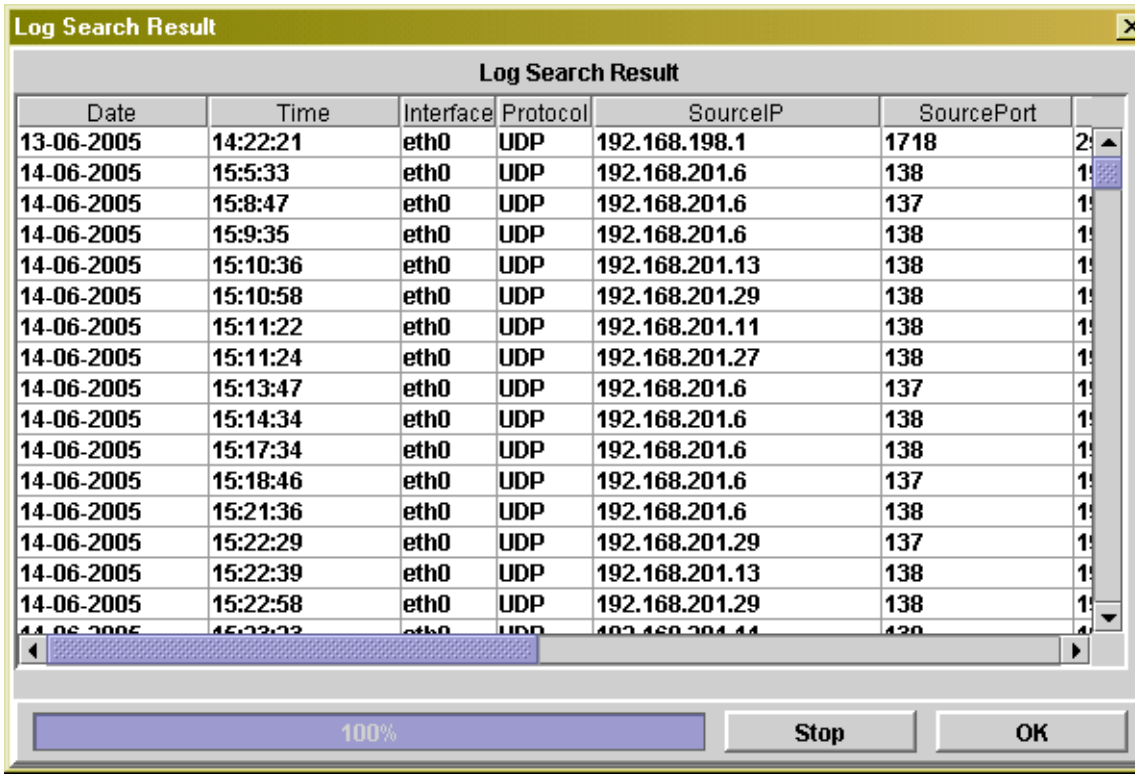


Figure P-4 Log Search Result

A unique name will be assigned to each search criteria. Criteria's already searched will be displayed in the **Previous Search Criteria** combo box as shown in the following **Firewall Log Search** screen.

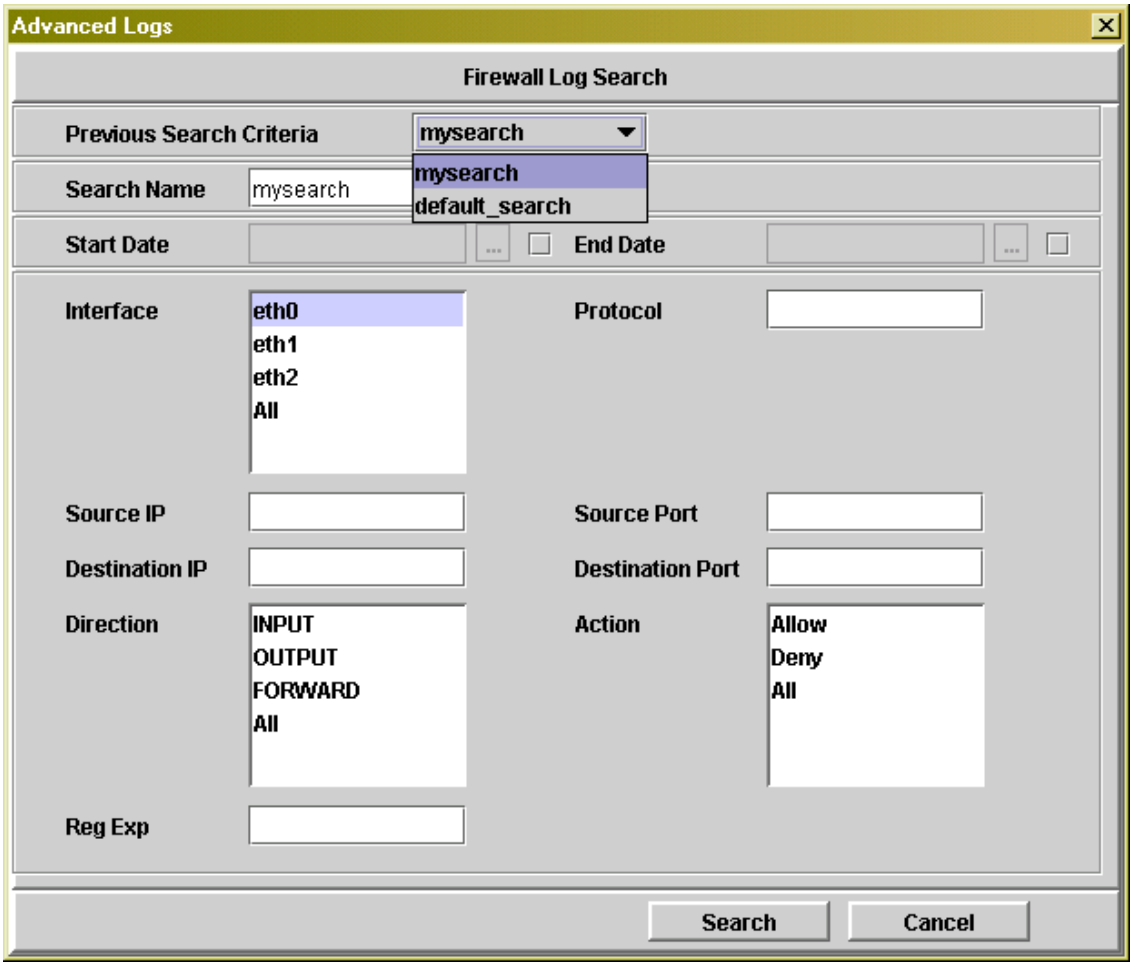


Figure P-5 Firewall Log Search

Selecting any Previous Search Criteria will load the search criteria information in the corresponding fields in the **Firewall Log Search** screen.

System Log Search

To navigate to the **System Log Search** screen,

- Click **Firewall logs** -> **System Log Search**

The following **System Log Search** screen appears

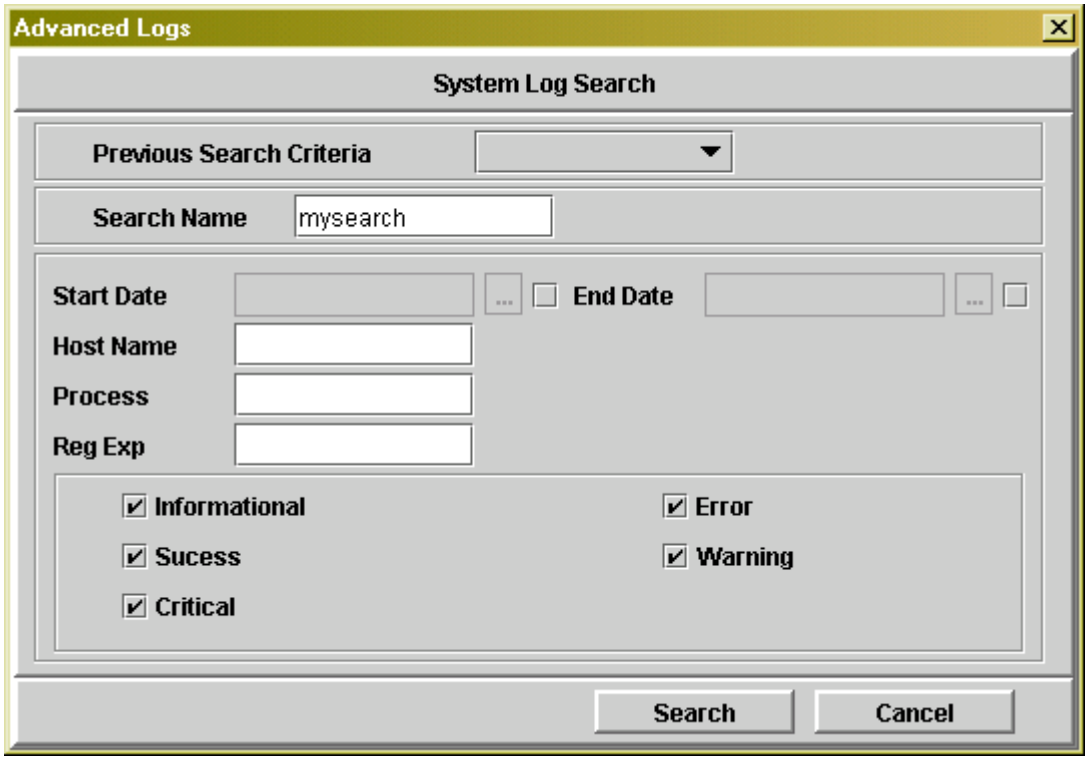


Figure P-6 System Log Search

To perform a **System Log Search,**

- Enter all the search criteria information in the fields provided in the **System Log Search** screen
- Click **Search** button

The following **Log Search Result** screen appears

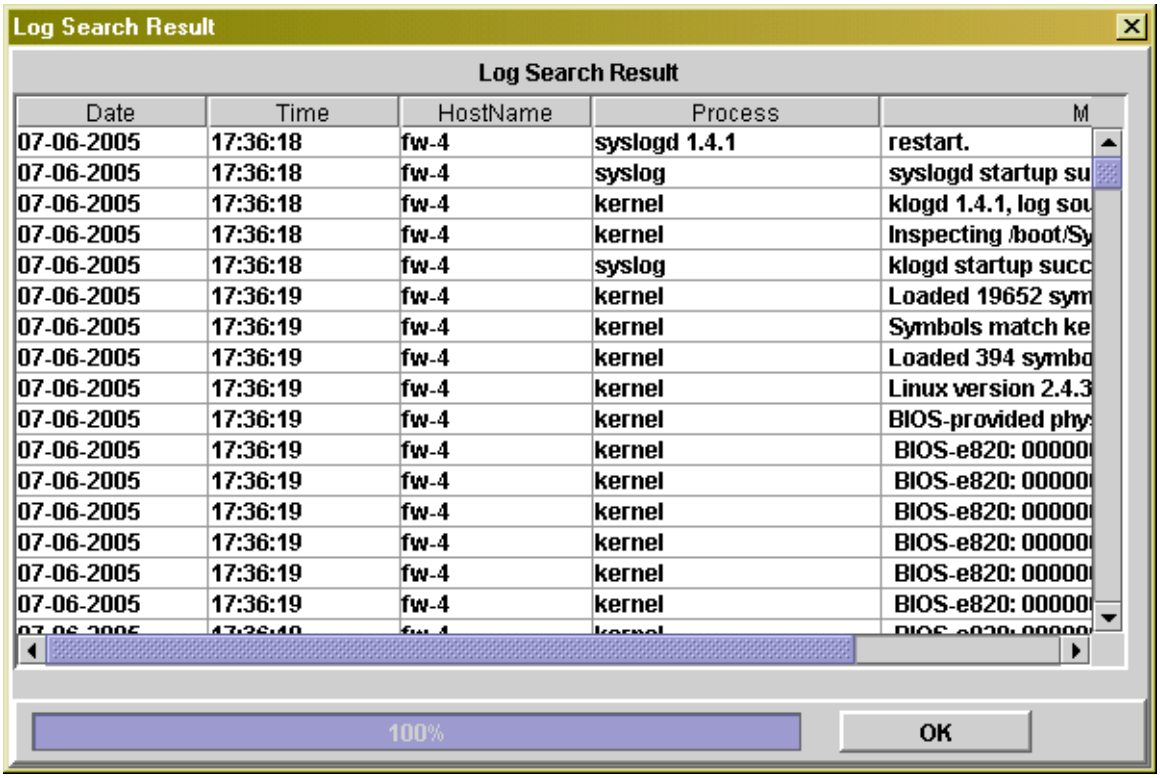

Log Search Result
Log Search Result
Date
Time
HostName
Process
M
07-06-2005 17:36:18 fw-4 syslogd 1.4.1 restart.
07-06-2005 17:36:18 fw-4 syslog syslogd startup su
07-06-2005 17:36:18 fw-4 kernel klogd 1.4.1, log sou
07-06-2005 17:36:18 fw-4 kernel Inspecting /boot/Sy
07-06-2005 17:36:18 fw-4 syslog klogd startup succ
07-06-2005 17:36:19 fw-4 kernel Loaded 19652 sym
07-06-2005 17:36:19 fw-4 kernel Symbols match ke
07-06-2005 17:36:19 fw-4 kernel Loaded 394 symbo
07-06-2005 17:36:19 fw-4 kernel Linux version 2.4.3
07-06-2005 17:36:19 fw-4 kernel BIOS-provided phy
07-06-2005 17:36:19 fw-4 kernel BIOS-e820: 00000
07-06-2005 17:36:19 fw-4 kernel BIOS-e820: 00000
07-06-2005 17:36:19 fw-4 kernel BIOS-e820: 00000
07-06-2005 17:36:19 fw-4 kernel BIOS-e820: 00000
07-06-2005 17:36:19 fw-4 kernel BIOS-e820: 00000
07-06-2005 17:36:19 fw-4 kernel BIOS-e820: 00000
100%
OK

Figure P-7 Log Search Result

A unique name will be assigned to each search criteria. Criteria's already searched will be displayed in the **Previous Search Criteria** combo box as shown in the following **System Log Search** screen.

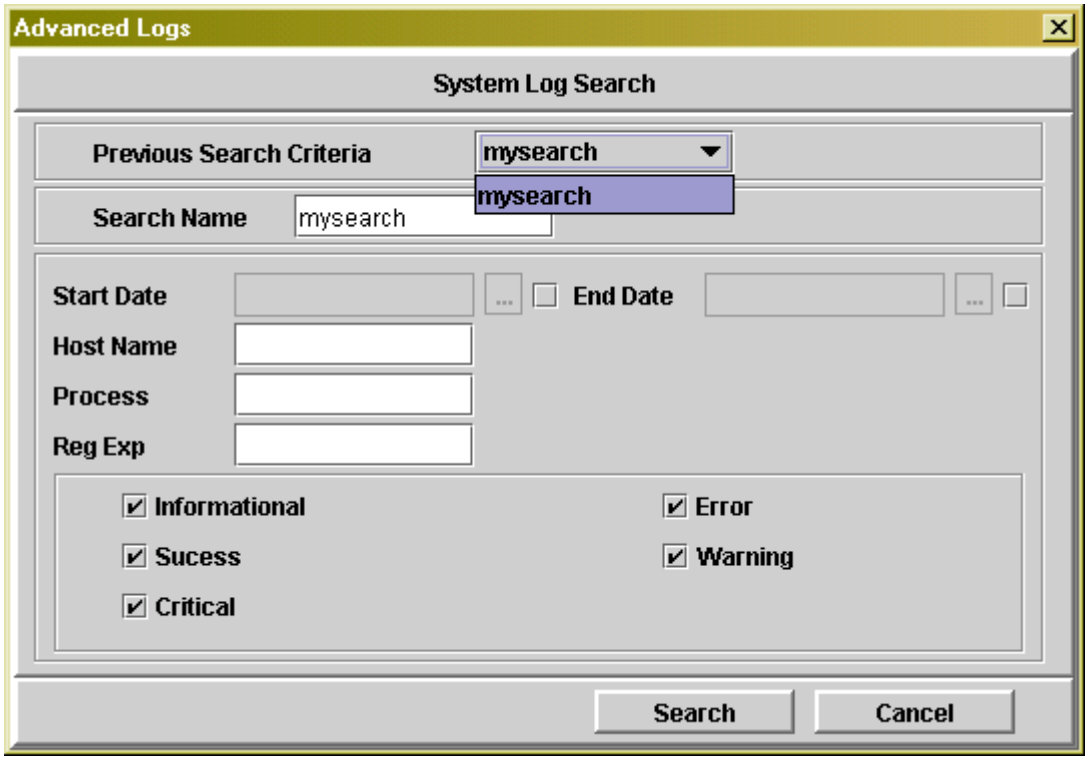


Figure P-8 System Log Search

Selecting any **Previous Search Criteria** will load the search criteria information in the corresponding fields.

Trustix™

Appendix Q

Static Routing

To navigate to the **Static Routing** screen,

- Click **Firewall** -> **Routing Entry**

The following **Routing Entry** screen appears

The **Routing Entry** screen initially displays the default route available in the firewall. You can also add or remove static routing to the firewall.

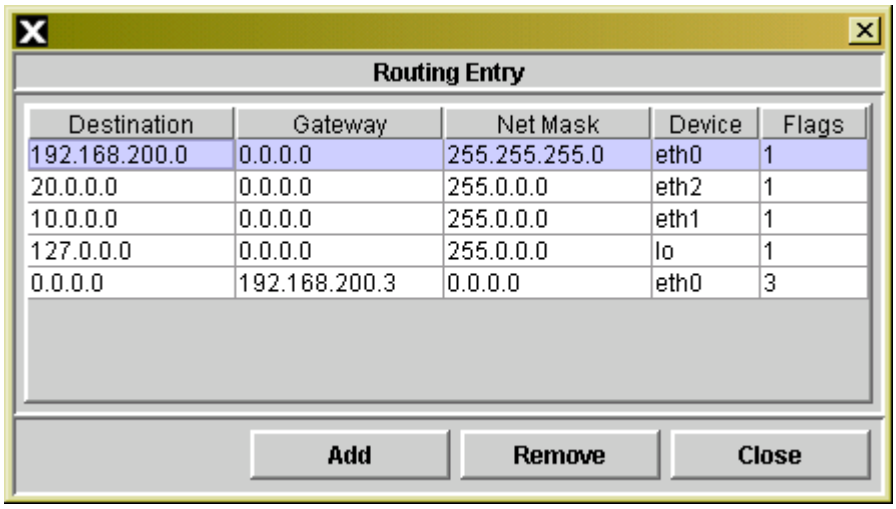


Figure Q-1 Routing Entry

Adding Static Routing

To add a route to the firewall,

- Click **Add** button

The following **Routing Entry** screen appears

Figure Q-2 Add Routing Entry

- Enter the destination address in the **Destination** field
- Enter the gateway address in the **Gateway** field
- Enter the net mask address in the **Net Mask** field
- Enter the device name in the **Device** field
- Click **OK** button

Removing Static Routing

To remove a route from the firewall,

- Select a route to be removed from the routing table
- Click **Remove** button

Note: It is not possible to remove the default route entries present in the firewall server. It is only possible to remove the routing entries which are manually added.

Trustix™

Appendix R

Firewall Policies within a Subnet

To expand a subnet, follow the steps given below:

- Right click on a subnet
- Select **Expand/Iconize** option.

You can see the subnet expanded to the full zone where it present.

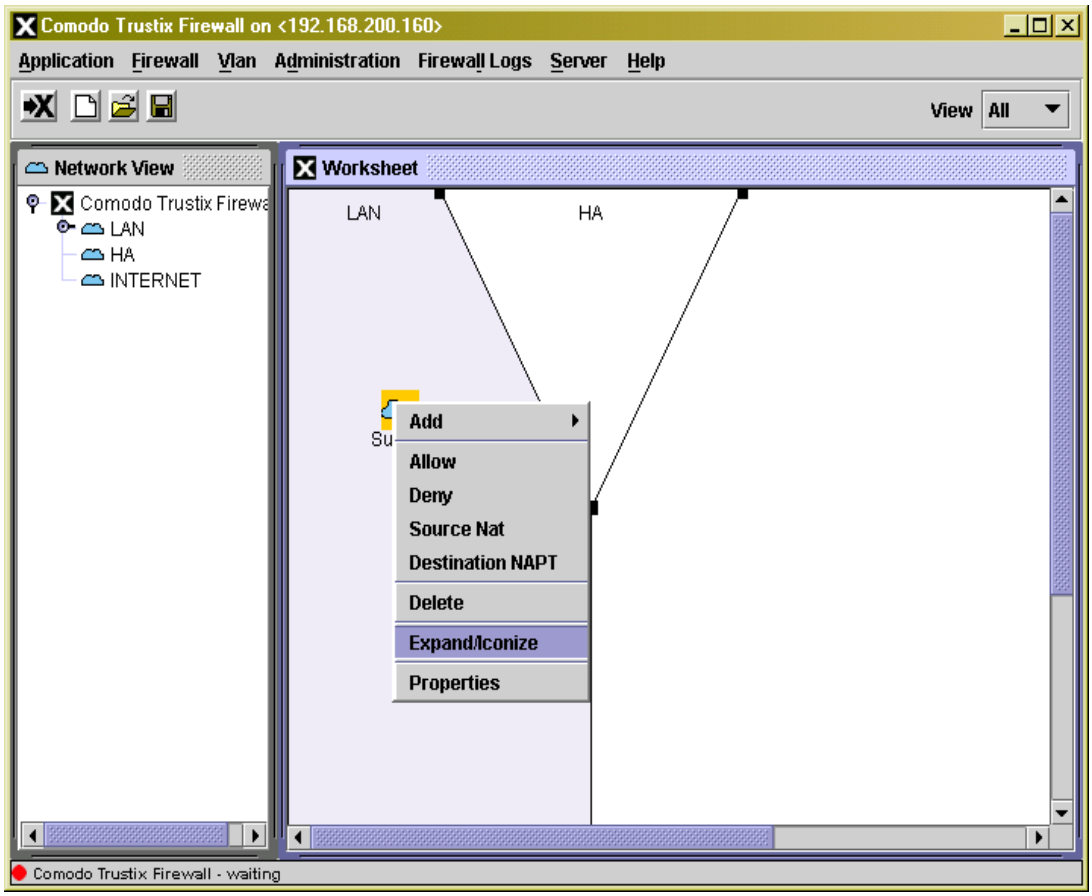


Figure R-1 'ConfigureHA' initial setup screen

Note: Now, you can add any number of entities and all the rules are applicable for the entities.

To view Subnet as an entity, follow the steps given below:

- Right click on the subnet zone
- Select **Expand/Iconize** option

Trustix™

Appendix S

Xsadm console menu option from Java GUI

The Xsadm console consists of various features discussed below. These features are also available in Java Client.

Change System Password

To navigate to **System Password** section,

- Click **Administration** -> **Change System Password**

The **System Password** screen appears.

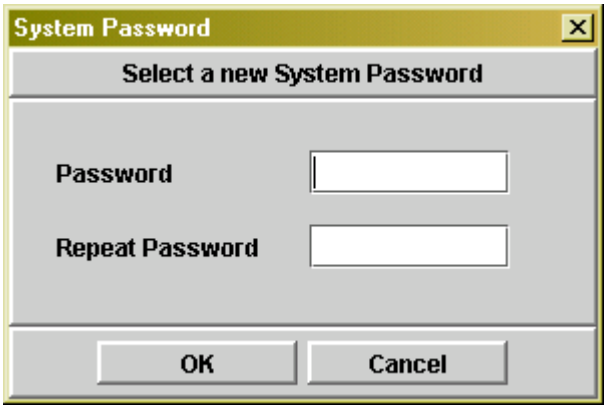


Figure S-1 Select a new System Password

Note:

- **Password** and **Repeat Password** fields are mandatory
- Password must be at least 6 characters long
- **Password** and **Repeat Password** must be same

Blocked Admin Hosts

To navigate to **Blocked Admin Hosts** section,

- Click **Administration ‡ Block**

The **Firewall Blocked Hosts** screen appears

Figure S-2 Firewall Blocked Hosts

To unblock a host, follow the steps given below:

- Select a blocked host from **Blocked Admin Host** field
- Click **Re-enable**
- Click **OK**

Configure Admin Host Blocking

To configure **Admin host blocking**, follow the steps given below:

- Click **Administration -> Change System Password**

The **Admin Host Lockout Setup** screen appears

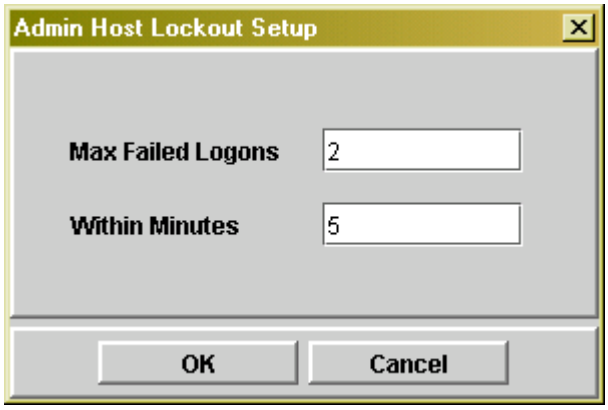


Figure S-3 Admin Host Lockout Setup

- Enter the necessary information
- Click **OK**

Enable Traffic Control

If the traffic control is already disabled then, **Enable Traffic Control** option will be available in **Administration** menu.

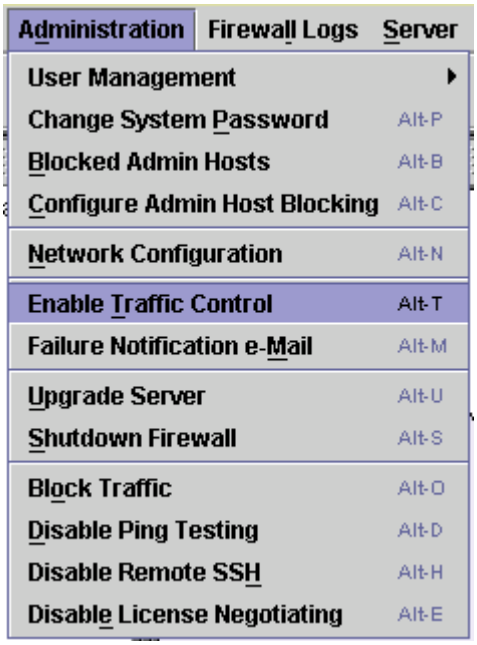


Figure S-4 Administration Menu

To enable traffic control, follow the steps given below:

- Select **Enable Traffic Control** option

The **Enable Traffic Control** screen appears

Figure S-5 Enable Traffic Control

- Click **OK**

Disable Traffic Control

If the traffic control is already enabled then, **Disable Traffic Control** option will be available in the **Administration** menu.

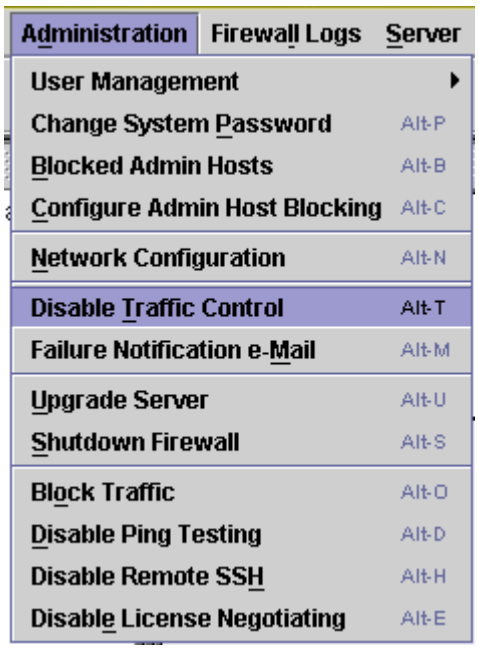


Figure S-6 Administration Menu

To disable traffic control, follow the steps given below:

- Select **Disable Traffic Control** option

The **Disable Traffic Control** screen appears

Figure S-7 Disable Traffic Control

- Click **OK**

Failure Notification e-Mail

To send e-mail for failure notifications, follow the steps given below:

- Select **Failure Notification e-Mail** option

The **E-Mail Address** screen appears

- Enter the e-mail addresses
- Click **OK**

Note: The **To** address field is mandatory.

Upgrade Server

To upgrade the Firewall Server, follow the steps given below:

- Select **Upgrade Server** option

The **Server Upgrade** dialog box appears

- Click **OK** to upgrade the firewall server

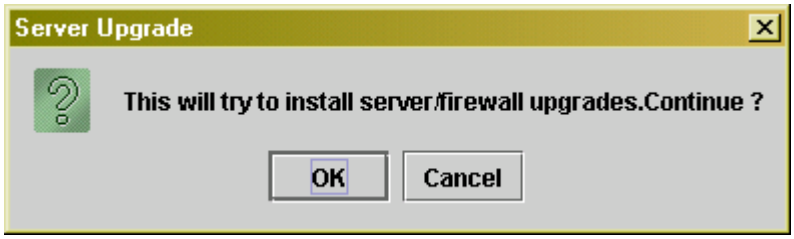


Figure S-8 Server Upgrade

Shutdown Firewall

To shutdown the firewall, follow the steps given below:

- Select **Shutdown Firewall** option

The **Shutdown Firewall** dialog box appears

- Click **OK** to shutdown firewall

Figure S-9 Shutdown Firewall

Block Traffic

If the network traffic is already unblocked then, **Block Traffic** option will be available in the **Administration** menu.

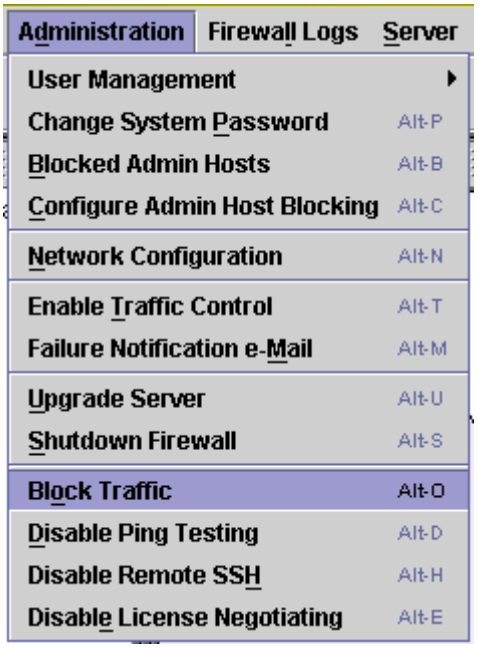


Figure S-10 Administration Menu

To block traffic, follow the steps given below:

- Select **Block Traffic** option

The **Block Traffic** dialog box appears

Figure S-11 Block Traffic

- Click **OK** to disable all network traffic through the firewall

UnBlock Traffic

If the network traffic is already blocked then, **Unblock Traffic** option will be available in the **Administration** menu.

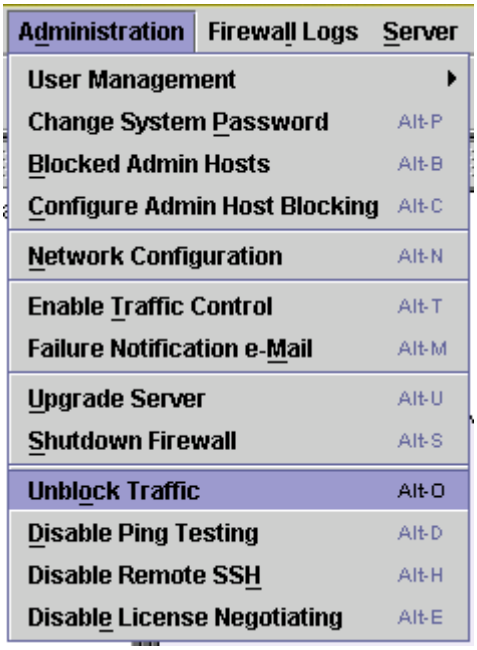


Figure S-12 Administration Menu

To unblock traffic, follow the steps given below:

- Select **Unblock Traffic** option

The **Unblock Traffic** dialog box appears

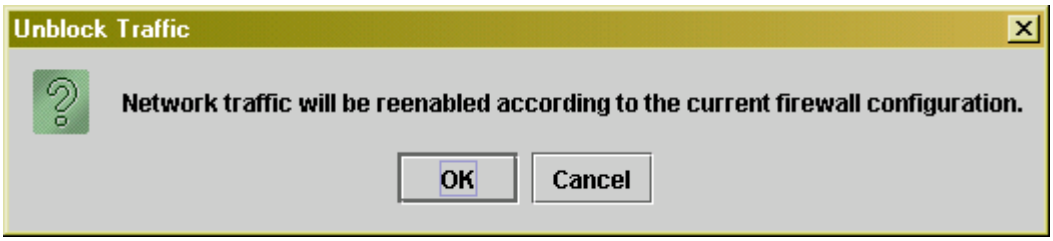


Figure S-13 Unblock Traffic

- Click **OK** to enable all network traffic through the firewall

Enable Ping Testing

If the ping testing is disabled in the firewall then, the **Enable Ping Testing** option will be available in the **Administration** menu

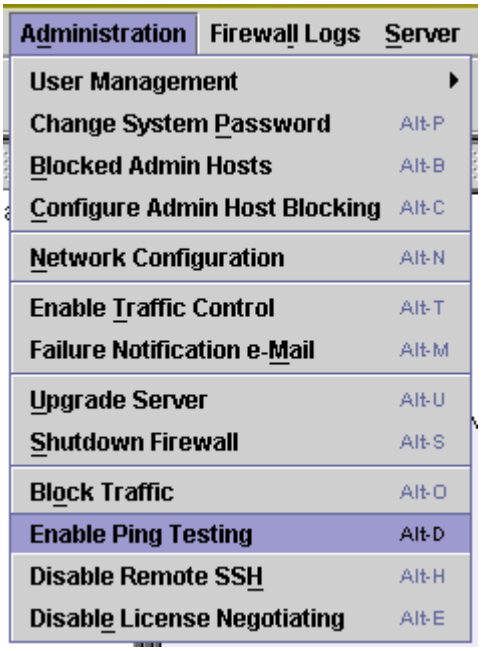


Figure S-14 Administration Menu

To enable ping testing, follow the steps given below:

- Select **Enable Ping Testing** option

The **Enable Ping Test** dialog box appears

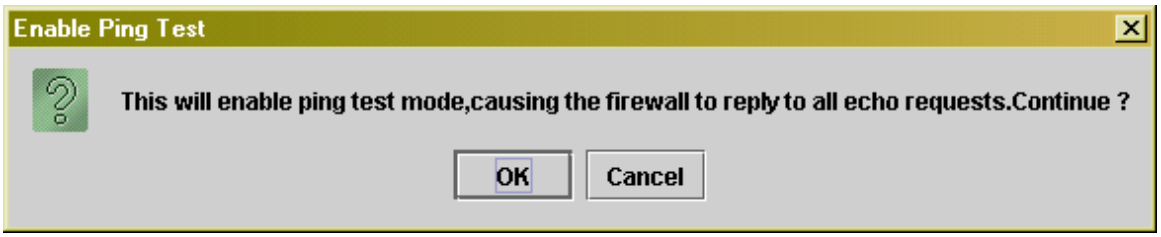


Figure S-15 Enable Ping Test

- Click **OK** to enable the ping testing in the firewall

Disable Ping Testing

If the ping testing is enabled in the firewall then, **Disable Ping Testing** option will be available in the **Administration** menu.

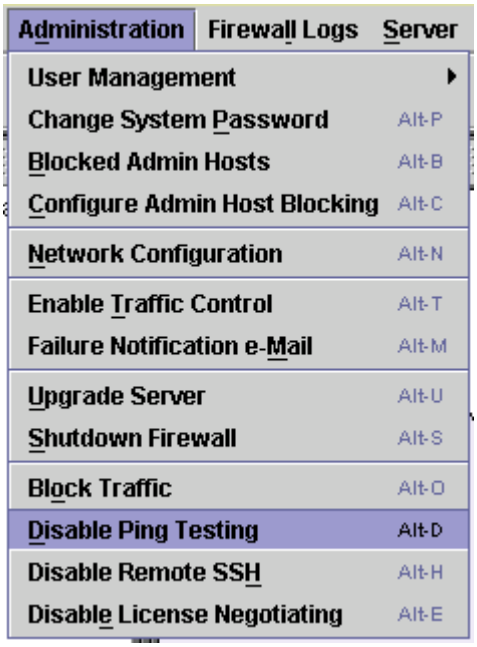


Figure S-16 Administration Menu

To disable ping testing, follow the steps given below:

- Select **Disable Ping Testing** option

The **Disable Ping Test** dialog box appears

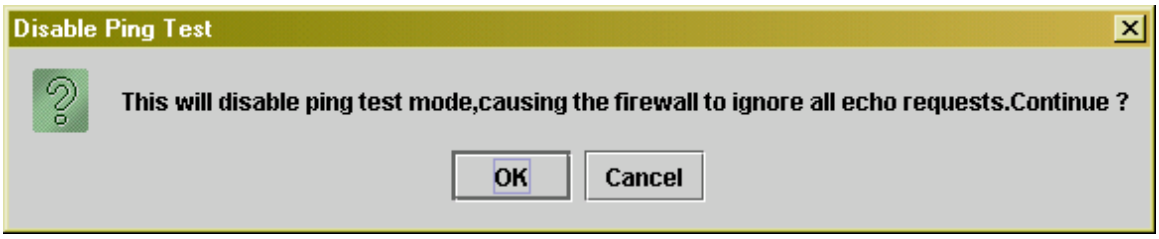


Figure S-17 Disable Ping Test

- Click **OK** to disable the ping testing in the firewall

Disable Remote SSH

If remote SSH is enabled in the firewall then, **Disable Remote SSH** option will be available in the **Administration** menu.

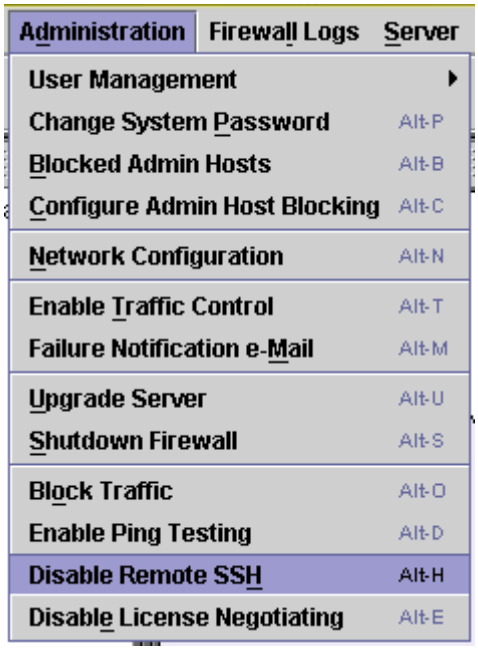


Figure S-18 Administration Menu

To disable remote SSH, follow the steps given below:

- Select **Disable Remote SSH** option

The **Disable Remote SSH** dialog box appears

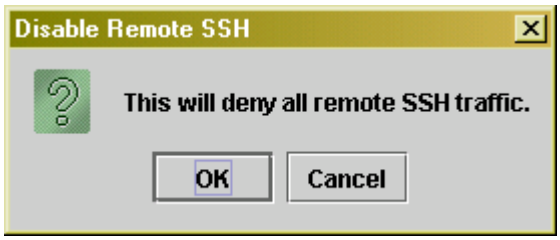


Figure S-19 Disable Remote SSH

- Click **OK** to disable remote SSH in the firewall

Enable Remote SSH

If remote SSH is disabled in the firewall then, **Enable Remote SSH** option will be available in the **Administration** menu.

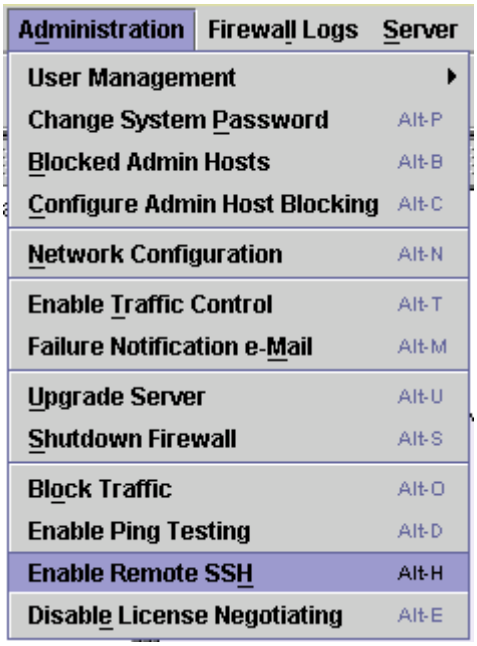


Figure S-20 Administration Menu

To enable remote SSH, follow the steps given below:

- Select **Enable Remote SSH** option

The **Enable Remote SSH** dialog box appears

Figure S-21 Enable Remote SSH

- Click **OK** to enable remote SSH in the firewall

Disable License Negotiating

If license negotiating is enabled in the firewall then, **Disable License Negotiating** option will be available in the **Administration** menu.

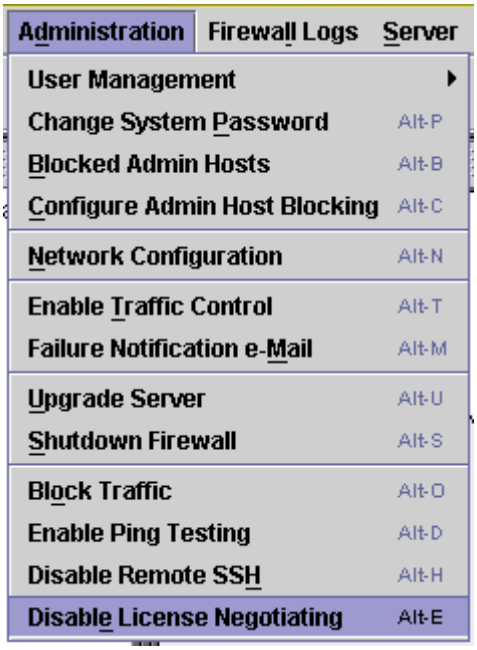


Figure S-22 Administration Menu

To disable license channel, follow the steps given below:

- Select **Disable License Negotiating** option

The **Disable License Channel** dialog box appears

Figure S-23 Disable License Control

- Click **OK** to disable the license channel in the firewall

Enable License Negotiation

If license negotiating is disabled in the firewall then, **Enable License Negotiating** option will be available in the **Administration**

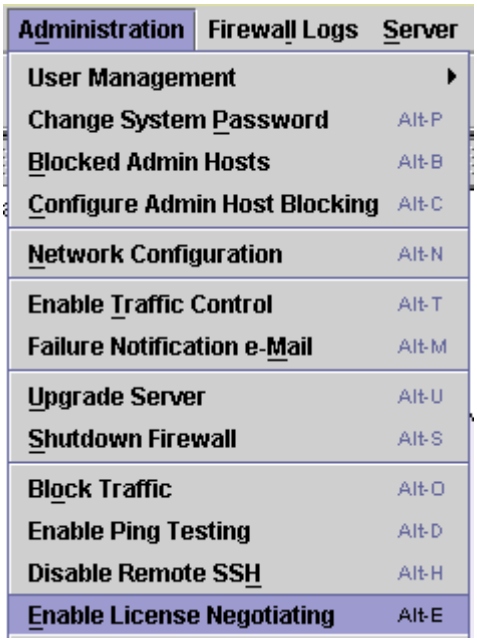


Figure S-24 Administration menu

To enable **Enable License Negotiating**, follow the steps given below:

- Select **Disable License Channel** option

The **Disable License Channel** dialog box appears

Figure S-25 Disable License Channel

- Click **OK** to disable the license channel in the firewall

Trustix™

Appendix T

User Management

To navigate to the User Management section,

- Click **Administration** -> **User Management**

The **User Management** section allows you to perform the following operations:

- New User
- Edit User

New User

To navigate to **New User** section,

- Click **User Management** -> **New User**

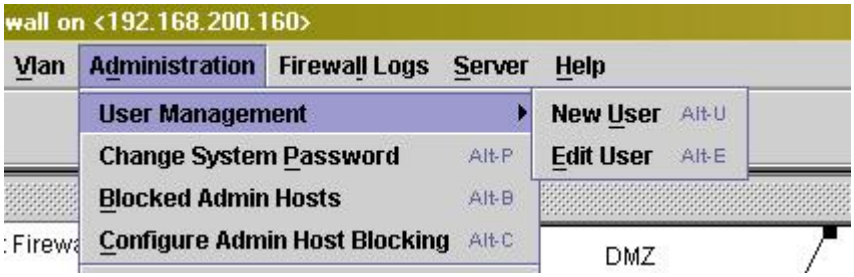


Figure T-1 Administration Menu

The **New User** screen appears

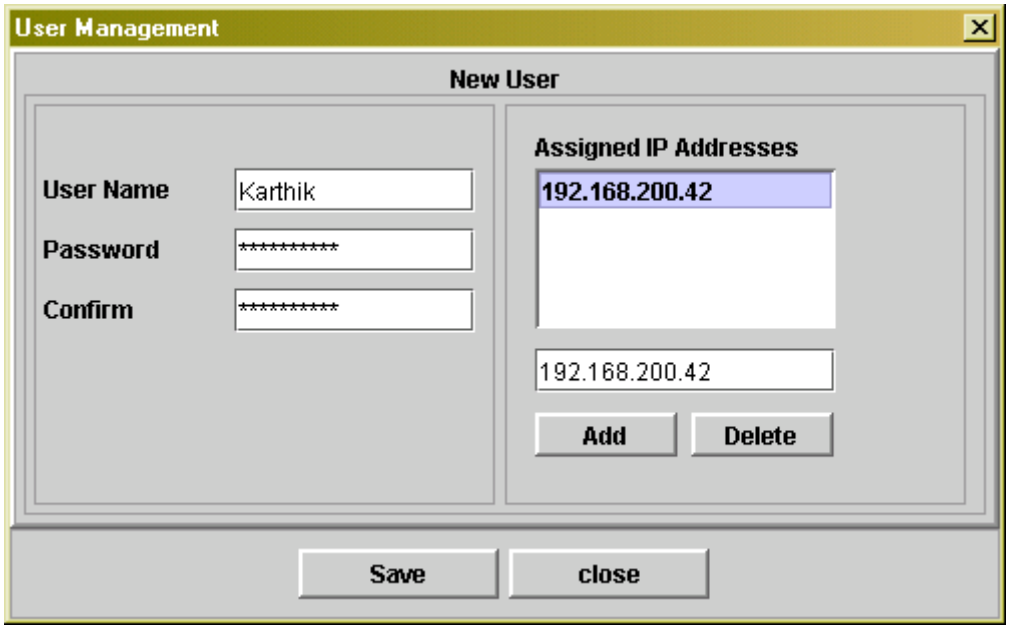


Figure T-2 New User

To add a new user, follow the steps given below:

- Enter the username in **User Name** field
- Enter password in the **Password** field
- Enter password again in **Confirm** field

Note: The password must contain minimum of 6 characters.

- Enter the IP address of the client machine from which you want to run the Java client in the **Assigned IP Addresses** field

Note: You can add more than one IP Address.

- Click **Add**
- Select the IP address that you wish to delete and then click **Delete**
- Click **Save**

Edit User

To navigate to **Edit User** section,

- Click **User Management ‡ Edit User**

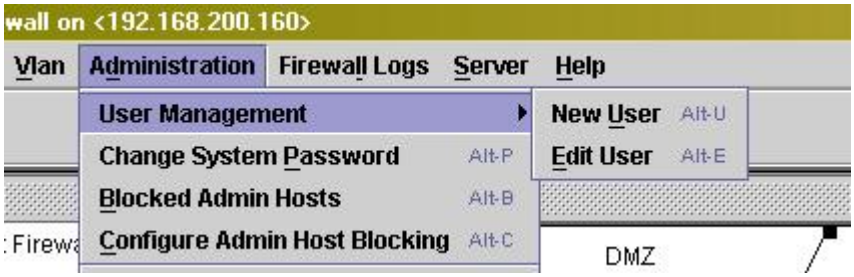


Figure T-3 Administration Menu

The **Edit User** screen appears

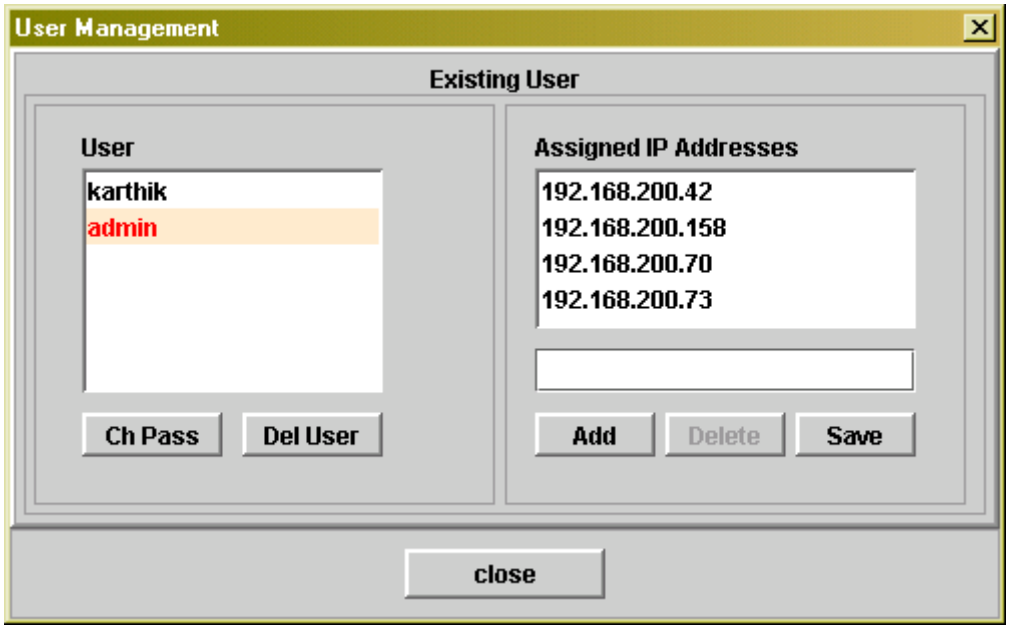


Figure T-4 Edit User

In **Edit User** section, you can perform the following operations:

- Delete User
- Delete any IP address assigned to a user
- Change Password

To delete a User, follow the steps given below:

- Select a user to be deleted from **User** field
- Click **Del User**

To delete any of the assigned IP addresses of a user, follow the steps given below:

- Select the IP address to be deleted from **Assigned IP Addresses** field
- Click **Delete**
- Click **Save** to save the changes in the firewall server

To change the password, follow the steps given below:

- Click **Ch Pass**

The **Change Password** screen appears

Figure T-5 Change Password

- Enter new password in **New Password** field
- Enter the new password again in **Confirm Password** field
- Click **OK**

Trustix™

Appendix U

High Availability

Concept

The Trustix Firewall can be set up in a fault-tolerant mode where automatic failover improves the availability of the firewall in the event of hardware or software failures.This functionality is called ***High-Availability (HA).***

HA is a Master-Slave firewall configuration with the default firewall zones and a dedicated interface to send HA keep-alive messages. On the Master, all the network interfaces are enabled (a network interface is usually a Network Interface Card or ***NIC***.). On the Slave, only the HA interface is enabled and all other interfaces are disabled - thus giving up full control to the master.

When there is a failure in the Master, the Slave will assume all duties and services and will act as a Master. When the Master is restored, it will act as a Slave.

Backup

The Slave will periodically update itself with the important configuration files from the Master machine. The required configuration files which have to be updated is configured in the file /opt/xsentry/etc/habackup.cfg. Any new updatation can be added in this file.

Sample Scenario:

In the following example, we have two firewalls; one set as the Master and the other as a Slave. Their interface addresses are as follows:

Master firewall machine:
eth0: 192.168.1.2/24 (Zone: LAN)

eth1: 192.168.2.2/24 (Zone: WAN)
eth2: 192.168.3.1/24 (Zone: HAzone)

Slave firewall machine
eth0: 192.168.1.2/24 (Zone: LAN)
eth1: 192.168.2.2/24 (Zone: WAN)
eth2: 192.168.3.2/24 (Zone: HAzone)

Note: For the purposes of this document, the terms *NIC* and *eth* are interchangable.

See **Fig H-1** below for a topology of this setup.

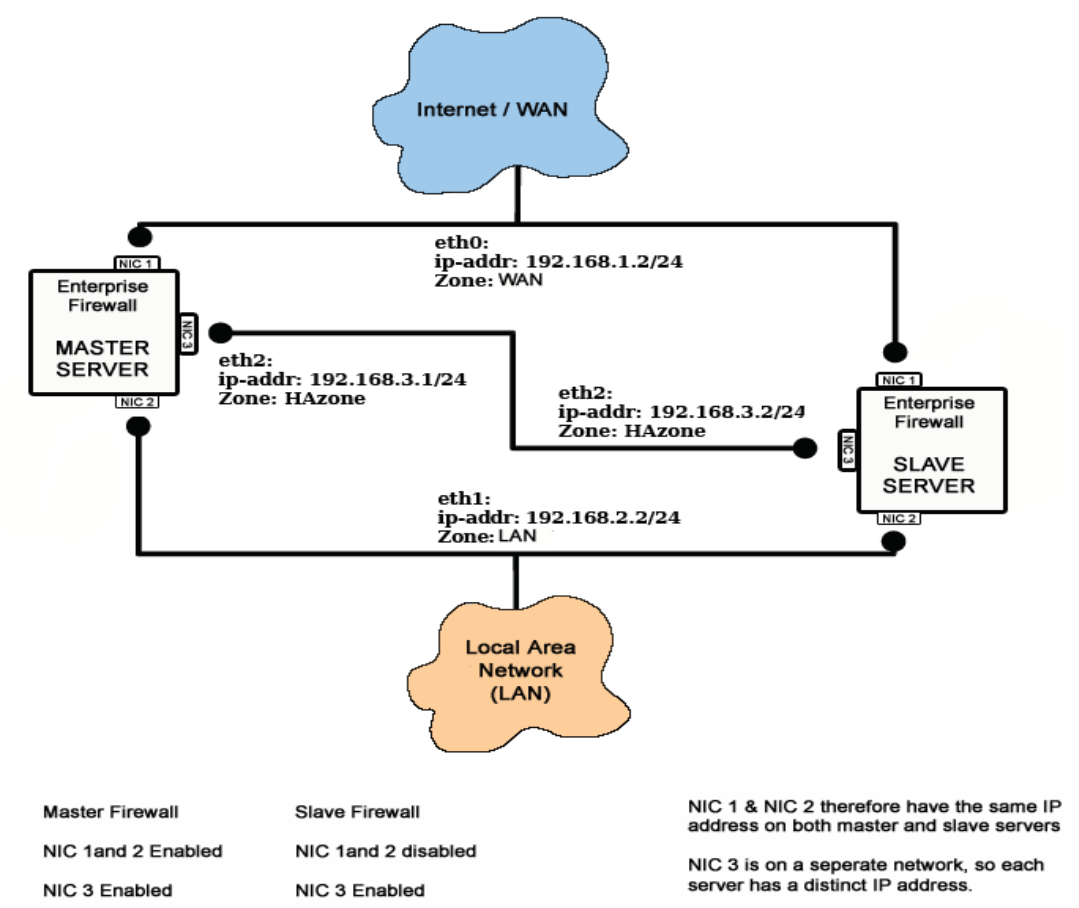


Figure H-1 Fault tolerant firewall setup

Figure H-1 shows a typical fault-tolerant configuration for the Trustix Firewall. It is a Master-Slave firewall configuration with three zones - Internet, LAN and HA. A Master-Slave relationship exists when, in the event of Master failure, the Slave assumes the duties of the Master.

The Network Interface Cards 1 and 2 have equal addresses on the Master and Slave servers. On the Master firewall, all network cards are enabled. On the Slave firewall, only NIC 3 is enabled. This network card is used by the Slave to monitor the Master. If the Master fails, and stops sending signals to the Slave, the Slave will activate all its network cards, acquire the Master's IP addresses take over all the traffic from the Master.

Configuring High Availability

Prerequisites

Set up the Master and Slave firewalls according to the rules outlined above. Ensure the NIC cards are not connected in network while configuring to avoid any inconsistencies. Alternatively, configure each machine whilst the other is shutdown.

To navigate to the **High Availability** screen,

- Click **Server** -> **High Availability**

The following **High Availability** screen appears

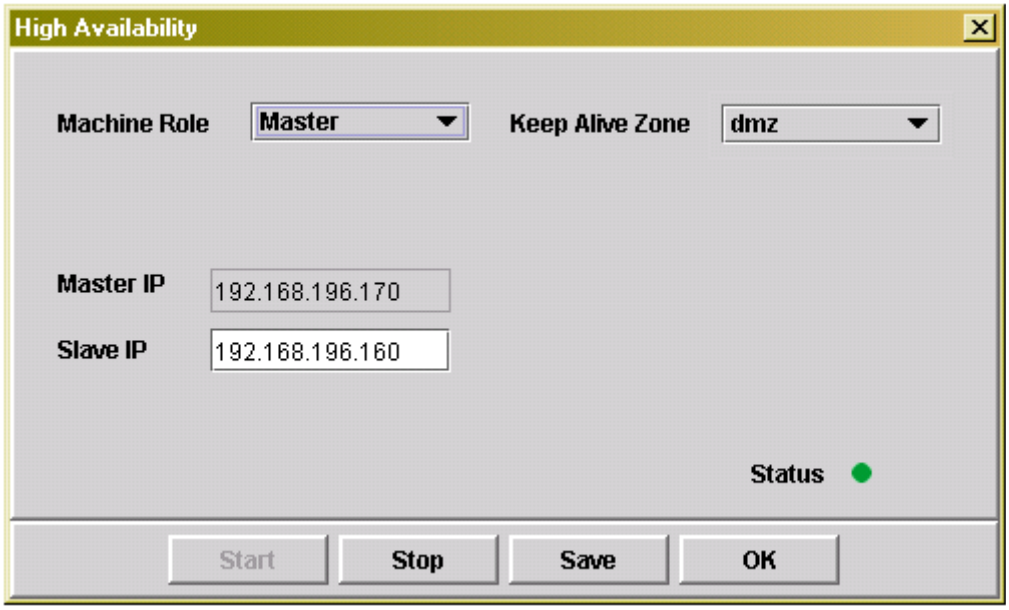


Figure U-1 Master Configuration

Activating High Availability from Java GUI

To activate High Availability in **Master** machine, follow the steps given below:

- Enter all the necessary information
- Click **Save** to save the High Availability configuration in the server
- Click **Start** to start the High Availability

To activate High Availability in **Slave** machine,

- Shutdown the master firewall server
- Start the slave machine
- Connect the Java client to the Slave machine
- Enter the necessary information
- Click **Save** button to save the configuration in the slave machine
- Click **Start** to start the High Availability

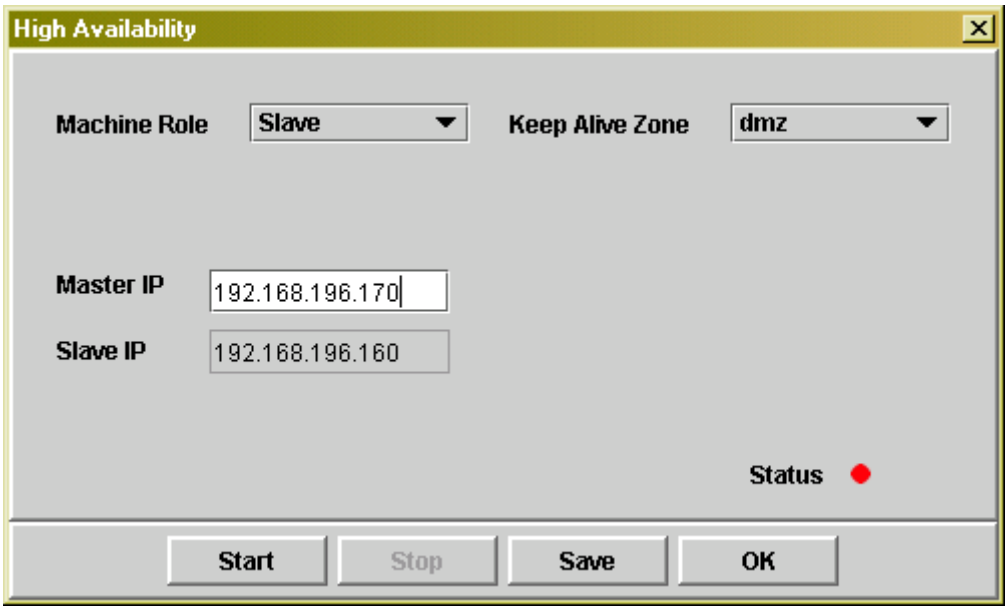


Figure U-2 Slave Configuration

Trustix™

Index

A

Activating Rules 93
Add 84
add
- host 83
- host folder 86
- node 82
- server 84
- server class 85
- service 83
- subnet 85

Address mask 117
Alerts 167
appliances 42
ARP Proxy 179
AUTH 117

B

block traffic 67

C

configuration
- firewall console 44
- LAN client 106

configure
- XSentry client 81

Configure Networks 62
configure networks 45
Configuring the Firewall Console 44
console tools 125
console-tools 125

D

default gateway 46, 62
Deleting Rules 93
Destination Unreachable 117
DHCP Common 159
DHCP Relay 163
DHCP Server 159
digital certificate 127
- revoke 136

DMZ 2
DNS 117

E

edit services 102
Entities 8
entity 8

F

Firewall 1
firewall
- appliance 42
- rules 8

Firewall Server 32
FTP 117

fwlogwatch 125

G

Gateway 5
gateway 5
  default 46
Generic UDP 117

H

High-Availability 203
Host 83
Host Folder 86
host folder 9
Host folders 9
host node 9
Host nodes 9
HTTP 118
HTTPS 118

I

IMAP4 118
installation
  firewall server 33
  prerequisites 31
  XSentry client 50
Internet 2
IP address 4
  dynamic allocation 10
IP-address 3
IP Pools 160
IPSec 6, 7
IRC 118

L

LAN 2
LAN Client Configuration 106
LAN Interface 45
LAN interface 45
License Negotiation 207
Lotus Notes 118

M

MAPI 150
Menu Bar 72
menu bar 72

N

Netbios 118
Netsceen 133
Network Device 3
network device 3
  locate 49
Network View 79
network view 79
NNTP 118
Node 8, 82
node 8
  add 82
  properties 89, 92
  remove 89

O

overview
  firewall 27

P

Parameter problem 119
passphrase 130
PGPNet 133
ping 67, 118
POP3 118
port forwarding 5
PPTP 118
Prerequisites 31
priority 113
putty ssh 115

R

Redirect 119
remote SSH 68
Remove 84
remove node 89

Revoking Certificates 136
Road Warrior 9
road warrior 9, 129
Router advertisement 119
Router solicitation 119
Routing 4
routing 4
Rule Examples 93
Rules 7
rules
activate 93
delete 93
examples 93
priority 113
set 90

S

Server 84
Server Class 85
Server class 9
server class node 9
server node 9
Server nodes 9
Service 83
Service node 8
service node 8
services
edit 102
port range 120
predefined 117
set rules 90
Setting Rules 90
Shell 50
shell 50
SIMAP 118
SMTP 119
Source quench 120
SSH 119
In MS Windows 115
Static Host 161
Subnet 85
subnet node 9
Subnet nodes 9
Subnetting 5
subnetting 5
Support 157
support 157
System Password 57
system password 59, 61

T

TCP/IP 3
TELNET 119
Time exceeded 120
Timestamp 120
toolbar 75
Traffic Shaping 145

U

upgrade 123
upgrades 123
Users 60
users 60

V

Virtual LAN 137
VPN 6, 119, 127
clients 133
VPN client 136

W

Windows Directory Service 119
Windows Networking 119
work area 76
Worksheet 76
worksheet 76

X

XML 73
XSentry client 137

Z

zone 8
Block Traffic 200